



UNDERSTANDING PAYMENTS

A MERCHANT'S GUIDE TO CREDIT CARD PROCESSING

helcim

CONTENTS

- 4 A Note from the Helcim Team
- 5 Introduction
- 7 The Road to Understanding Payments Starts Here
- 8 Benefits of Accepting Credit Cards

01

HOW DOES IT ALL WORK?

- 11 The Credit Card Ecosystem
- 11 The Card Brands
- 12 The Cardholders and Issuers
- 13 American Express
- 13 The Merchants and Processors
- 14 The Credit Card Transaction Process
- 17 Batch Settlement

02

CHOOSING A MERCHANT ACCOUNT PROVIDER

- 19 What Does Applying for a Merchant Account Mean?
- 19 How to Sign Up and Why Underwriting Applies to Credit Card Processing
- 21 Provider Types
- 21 The Bank Processors
- 22 MSPs and ISOs (Resellers)
- 23 High Risk Payment Processors
- 24 Associations, Chambers and Lobby Groups
- 24 Retailers Selling Merchant Services
- 25 The Payment Facilitators
- 25 The Software Platform

03

FEES RATES & PRICING

- 27 What is Interchange Rate?
- 27 When Does the Interchange Fee Apply?
- 27 Where Can I Find a List of Interchange Rates?
- 28 Why Do I Need to Know What It Is?
- 28 What Are Payment Processing Rates Made Up Of?
- 29 Types of Processing Pricing
- 29 Flat Rate Pricing
- 30 Tiered Pricing
- 31 Differential Pricing
- 32 Interchange Plus
- 33 Understanding Additional Fees Related to Credit Card Processing
- 33 Monthly Minimums
- 33 Statement Fee & Admin Fees
- 33 Quarterly Fees & PCI Fees
- 33 PCI Non-Compliance
- 33 Setup & Application Fees
- 33 Early-Termination, Contract Closure & Leasing Fees
- 34 Monthly Fee
- 34 International Cross-Border Fees
- 34 Bank Account Change/Business Name Change
- 35 NSF Fee
- 35 Chargeback Fee
- 35 Voice Authorization Fee



04

EQUIPMENT & SOFTWARE

- 37 Solutions for Card-Present Transactions
- 38 Credit and Debit Terminals
- 39 Card Readers
- 40 In Store Point of Sale System
- 40 Understanding Chip Cards
- 41 Using EMV to Reduce Liability
- 41 Card-Present vs. Keyed
- 41 Near Field Communication
- 42 Solutions for Card-Not-Present (Online) Transactions
- 42 Virtual Terminal
- 42 Payment Pages
- 43 Gateway API
- 44 Third Party Software Integrations
- 44 Software

05

PROCESSING PAYMENTS

- 46 Card-Present vs Card-Not-Present
- 47 Transaction Types
- 47 Purchase
- 47 Pre-Authorization
- 47 Capture
- 48 Void
- 48 Refund
- 48 Verify
- 48 Approvals
- 49 Types of Credit Card Declines
- 50 Tips for Dealing with Declines
- 50 What is CVV
- 51 What is AVS
- 52 AVS Response Codes
- 53 Batches and Settlements
- 53 The Settlement
- 54 Gross Settlements vs. Net Settlements

06

RISK FRAUD & PCI

- 56 Understanding the Risks
- 56 Risks for Issuing Banks
- 56 Risks for Acquiring Banks / Processors
- 57 Risks for Merchants
- 57 Cardholder Protections & Risk For Your Business
- 58 Balancing Fraud and The Flow of Commerce
- 58 Merchant-Fraud
- 58 Fraud and Other Risks Merchants Face
- 58 Stolen Credit Cards
- 59 Friendly Fraud
- 60 Chargeback Fraud
- 60 Authorization Error
- 60 Customer Dispute / Chargeback
- 60 Issuer Dispute
- 60 Stolen Credit Card
- 61 Chargebacks
- 63 Chargeback Process
- 65 Fighting a Chargeback
- 65 Chargeback Arbitration
- 66 Protecting Your Business from a Chargeback
- 66 How to Evaluate the Legitimacy of a Transaction
- 70 PCI Compliance
- 70 Who Does it Apply to?
- 70 Who Sets the Standard and Who Enforces it?
- 70 Why Do I Have to be Compliant?
- 70 My Provider Is Compliant, Does that Mean I'm Compliant?
- 71 Becoming PCI Compliant
- 72 PCI Compliance and Non-Compliance Fees
- 72 PCI Compliance Fee (with a PCI Program)
- 72 PCI Compliance Fee (without a PCI Program)
- 72 PCI Non-Compliance Fee
- 73 Myths About PCI Compliance
- 75 Thank you
- 76 Getting to Know the Terms

A NOTE FROM THE HELCIM TEAM

The payment industry can be a rollercoaster ride. Making sense of all the fees, rates, and different ways to get paid can be overwhelming for business owners - especially when you think about how each decision you make can impact your bottom line.

At Helcim, our mission is to be the world's most loved payments company. Our guiding principles are simple: be honest, be fair, and be better. That's why Better Payments is our mantra. It's in our DNA to be the best we can for business owners everywhere.

That means committing to excellent customer service, the most affordable pricing in the industry, and total transparency with our merchants.

As part of our continued effort to ensure we help merchants stay informed about the complexities of the payments industry, we've put together a comprehensive whitepaper called the *Merchant's Guide to Credit Card Processing*.

This guide is an extension of our firmly established tradition of posting our rates and fees clearly on our website, providing educational content in our Newsletter and Blog, and employing a merchant support team that's sole purpose is to help and inform anyone who reaches out to us.

This guide is just one way that we can remove the veil from the payments industry, and share our years of experience with readers like you.

Throughout the guide, you will notice play buttons on certain pages. These link out to videos or other information on the topic you're reading about. If you would like to learn more, simply click on the play button.

We encourage you to reach out to our friendly team of **Helcim Gurus** if you have any questions about how payment processing works, or how Helcim can help save our business time, money, and frustration.

Sincerely,

The Helcim Team

www.helcim.com



INTRODUCTION

Accepting credit cards has become an integral part of doing business in today's world. And while certainly not a system without flaws, the card networks connect millions of merchants with over a billion customers worldwide. Over 10,000 transactions per second are processed in real-time by [Visa](#) and Mastercard alone.

Customers' dependency on credit card networks was highlighted by the brief outage Visa experienced in Europe in June 2018. While the outage was only 5-hours long, it became national news as people were unable to board trains, buy groceries, shop online, pay suppliers, or book their next flight.

There's no denying that the world is becoming more dependent on the credit card networks as we inch closer to a cashless society. As a business owner, you should understand that your customers have expectations on how they can pay for your products or services. If you're going to offer your customers the ability to pay with credit cards, then it is important that you have a solid understanding of the industry and how payment processing works.

The goal of *Understanding Payments* is to give you an in-depth understanding of how credit cards work and how your business can accept credit cards while avoiding some of the pitfalls of the payment processing industry.

Payments Glossary

If you're new to credit card processing, there may be some terms in this document that you haven't come across before and may not be familiar with. There is a helpful glossary at the end of this guide that outlines many of the common industry terms.

The Road to Understanding Payments Starts Here

Although the payment industry can seem overwhelming at first, there are lots of great resources (like this guide!) to help you navigate the vast, evolving landscape of selecting a payment processor. This guide will help you get started, so you can be confident in your choice of credit card processor and help protect your business from potential risks associated with accepting credit cards.

Customers appreciate being able to pay for products or services using their preferred method, and by accepting credit and debit cards, you are giving them more options and increasing the likelihood that they will make a purchase from your business. The benefits of accepting credit cards definitely outweigh the potential risks, but by educating yourself, you will be more aware of what to watch out for and how to set your business up for a rewarding payment processing experience for both you and your customers.



Benefits of Accepting Credit Cards

Once your business reaches a certain size, accepting credit cards almost becomes a must. It benefits both your customers and your business for a variety of reasons, some of which may not be immediately obvious. Here are some of the reasons why your business would want to accept credit cards.

More Sales Opportunities

Accepting credit cards gives your customers more options to pay for purchases and also increases the likelihood that they will make a larger purchase. It's been shown that customers are more comfortable making larger purchases using their credit card, likely due to broad cardholder protections and a credit card's physical detachment from cash. Accepting credit cards also allows your business to set up an online store where customers from around the world can shop 24/7, giving your business significantly more opportunities to make sales.

Speed Up Your Transactions

Even compared to taking a cash payment and doling out change and receipts, credit card transactions are very fast, and they're only getting faster as new payment tools and technologies emerge. Authorizing a credit card takes only a few seconds, giving you more time to manage the rest of your business and help more customers. If your business accepts tap and NFC (Near Field Communication) payments, then the entire transaction can be reduced to a few seconds. This means faster checkouts and shorter lines for your customers, and more sales in less time for your business.

Trade Green for Going Green

As people seek out environmentally friendly practices for all aspects of their lives, accepting credit cards is one way businesses can reduce their environmental footprint. Going paperless helps businesses reduce their reliance on cash and paper for things like receipts, inventory lists, booking sheets, invoices, and spreadsheets. Since credit card transactions are essentially just data, it's possible to easily feed that data through an ever-growing number of business software applications and tools that allow you to send paperless receipts and invoices through e-mail, do all your accounting from the cloud, and manage your inventory and customer data all from your computer or phone.

Improve Your Cash Flow

Accepting credit cards affords you the ability to receive your deposits as quickly as a few hours or a few business days. Sure, "cash in hand" is cash in hand, but compared to checks which can take up to 30 days to clear, and invoices which can take up to 90 days to be paid, accepting credit cards gets money into your business's bank account faster.

Expand your market while staying competitive

Visa and Mastercard are international brands. By accepting these card types, you have access to customers in over 170 countries who are able to pay for your products or services with just a few clicks. Accepting credit cards also helps you keep up with your competition by meeting customer expectations for payment options – if you don't offer the payment type that they're expecting, then there's a greater chance they will go to another business that does. People are carrying less cash than ever before, and it's unlikely your business can afford to ignore this trend.





HOW DOES IT ALL WORK?

Credit cards are used every day to pay bills, purchase products online and in stores, and to pay for all types of services. However, many people do not fully understand how the payments are coordinated between a customer's credit card, the different banks involved, and the payment processor to allow for the quick and easy payment experience that we often take for granted.

The Credit Card Ecosystem

The Card Brands

Visa and Mastercard, the two biggest *card brands* in the world, are actually better understood as credit card *networks*. These credit card networks facilitate a system of real-time authorization and funding transfers between merchants (businesses), customers (cardholders), and their respective banks (acquiring bank and issuing bank respectively). The most popular networks in the US and Canada are Visa, Mastercard, Discover, and American Express.



▶ The Cardholders and Issuers

The customer who uses a credit card to make purchases is referred to as the *cardholder*.

A customer will usually enlist their local bank to apply for a credit card. It's the customer's bank that is responsible for issuing the credit card on behalf of the card brands. Therefore, the banks that provide credit cards are called *issuing banks* or *issuers*. Some examples of issuing banks including RBC, Bank of America, and TD. There are over 100,000 issuing banks worldwide. These issuers work in partnership with card brands such as Visa, Mastercard and Discover to offer co-branded cards with structured rewards, as well as ensuring that their cards follow network rules and will work wherever credit cards are accepted.

There is risk involved for issuing banks because they are extending credit to cardholders. If, for example, a cardholder is unable to pay their credit card balance, the loan must be written off. They are also responsible for compensating their customers if there are fraudulent transactions with their card. This risk is why issuing banks provide credit cards, and not the card networks themselves.



American Express

American Express (Amex) is another credit card brand and network. American Express is unique when compared to Visa and Mastercard, as not only are they a card brand with their own card network, but they are also the card issuing bank, and can take on cardholders directly. Many cardholders, especially businesses, will choose American Express credit cards as they often offer greater rewards and cardholder perks. However, this usually means higher processing fees for the merchant, which is why American Express may not be as widely accepted as Visa and Mastercard.

American Express offers the Opt-Blue program to make accepting their card easier and more affordable for merchants. The American Express Opt-Blue program offers three advantages over traditional Amex acceptance including instant Amex acceptance, combined bank deposits with other card brands, and Interchange plus pricing for better processing rates.

American Express does not provide equipment or services to merchants looking to accept their cards. If you want to accept Amex, then you must sign up with a credit card processor.

The Merchants and Processors

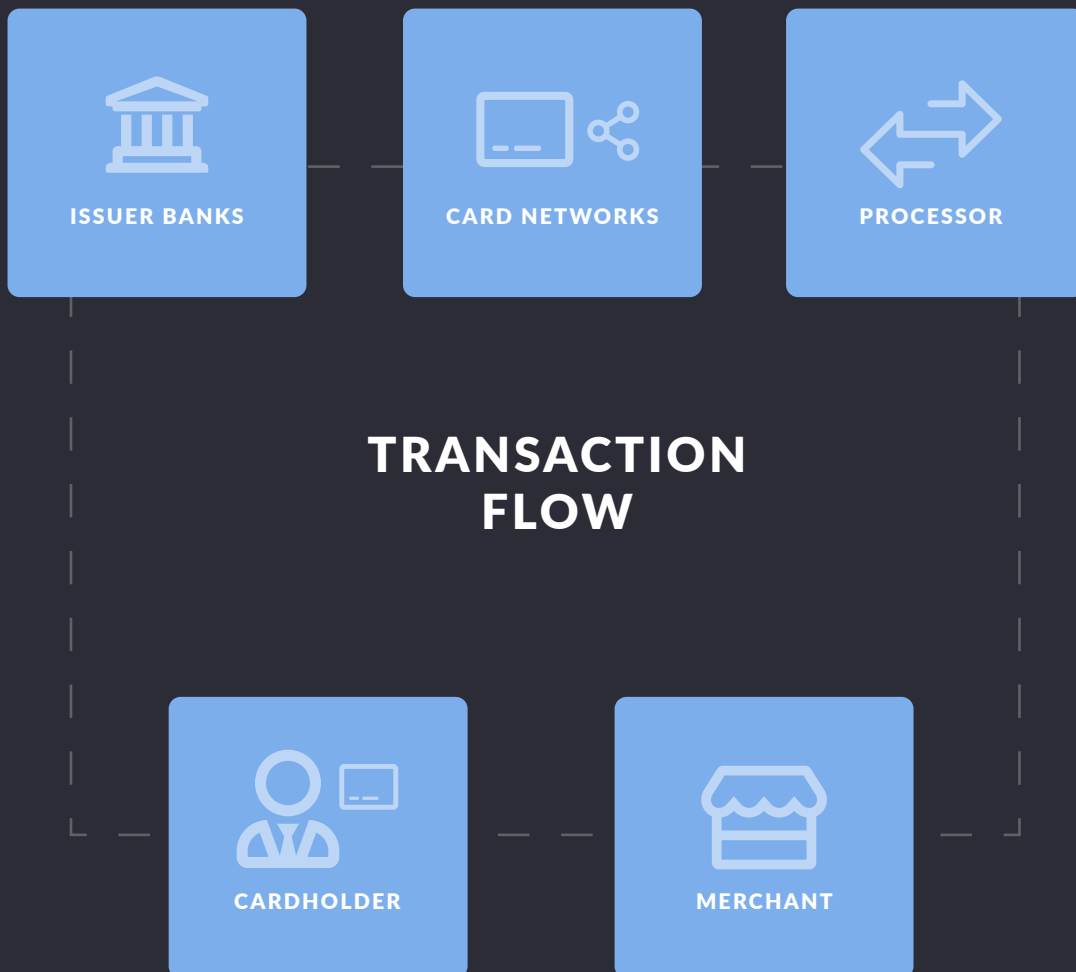
Just like cardholders, businesses like yourself who are looking to accept credit cards, referred to as merchants, do not contact Visa or Mastercard directly. Instead, businesses will sign up for a merchant account through a credit card processor. There are many processors available, examples include [Helcim](#), [Moneris](#), [Chase Paymentech](#), [First Data \(now Fiserv\)](#), [Global Payments](#), [PayPal](#), and others.

The processor will provide several functions to the merchant. First, they will register the business with the various card networks, so that they can accept all the payment types required. The processor essentially acts as the middleman between merchants and acquiring banks and will arrange for the processed funds to be deposited back into the merchant's bank account, typically within a few business days. The processor will also provide the merchant with the equipment and software needed to begin accepting credit cards. Finally, the processor will charge processing fees for their service, and usually provide customer service to help merchants in need.



The Credit Card Transaction Process

The diagram and notes below will walk you through a credit card transaction as it flows through the network.



- 1 A **cardholder** visits your location and pays for a transaction using their credit card through a payment terminal, which reads the information on the magnetic stripe or chip. For this example, we'll say that a Visa credit card was used.
- 2 Your payment terminal communicates with the **credit card processor** (let's say, Helcim) and sends information about the transaction, including the credit card details and the amount to be processed.
- 3 The **credit card processor** (Helcim) will detect what type of credit card it is (Visa) and communicates the transaction with the appropriate **card network** (Visa) via an encrypted authorization request.
- 4 The **card network** (Visa) determines the **issuing bank** (such as Citi Bank) and communicates the authorization request to them for review.
- 5 The **issuing bank** (Citi Bank) will either approve or decline the transaction based on whether the card is valid, if it has been flagged for fraud, and if the funds are available. If the criteria is met, it provides a response back to the **card network** (Visa) with an APPROVAL CODE.
- 6 The **card network** (Visa) then responds back to the **processor** (Helcim) with the approval information.
- 7 The **processor** (Helcim) responds back to your equipment, which then displays the approval message to the **cardholder**.
- 8 At the end of the night, the **card network** (Visa) will transfer the funds from the **issuing bank** (Citi Bank) to the **processor** (Helcim), which will then transfer the funds to the **merchant** (you).

What's amazing about this process is that most transactions go through all these steps in less than a second, providing real-time authorizations to merchants across the world. Visa alone processes thousands of transactions per second across its network, serving over 150 million transactions between cardholders and merchants worldwide every day.

The same process is employed for an ecommerce transaction, except that the customer enters their credit card information manually on your website, and the information then gets transmitted to the card brand by the merchant processor through a secure payment gateway.



Batch Settlement

Settling a *batch* triggers the process of delivering funds to the merchant and charging the customer's account. Here are the steps involved in a batch settlement.



Several transactions, usually within a 24-hour time frame, are aggregated (batched) together and transaction information is sent to the acquiring bank from the processor.



The acquiring bank then transfers the funds to the merchant's account and submits the transaction data to the card brand.



The card brand then settles the batch by issuing funds to the acquirer from the issuing bank.



The issuing bank then posts the transaction to the cardholder's monthly credit card statement.



CHOOSING A MERCHANT ACCOUNT PROVIDER

So, you've made the decision to accept credit cards, and now you're ready to start shopping for a payment processor to provide you with a merchant account. There are hundreds of providers and resellers to choose from – the local sales reps, Merchant Service Providers, Silicon Valley start-ups, and international banks are all options. The services they all offer vary widely, and so do their pricing and sales practices. The bottom line is that you're now faced with a difficult and complex decision that has real consequences for your business, so it's important that you educate yourself.

helcim

▶ What Does Applying for a Merchant Account Mean?

When you sign up for a *merchant account*, you are asking the payment processor to take a risk on behalf of your business. When the processor approves your account, they are confirming that they trust your business to honor the transactions that you process. If a business cannot honor their transactions, then the processor becomes liable for the loss.

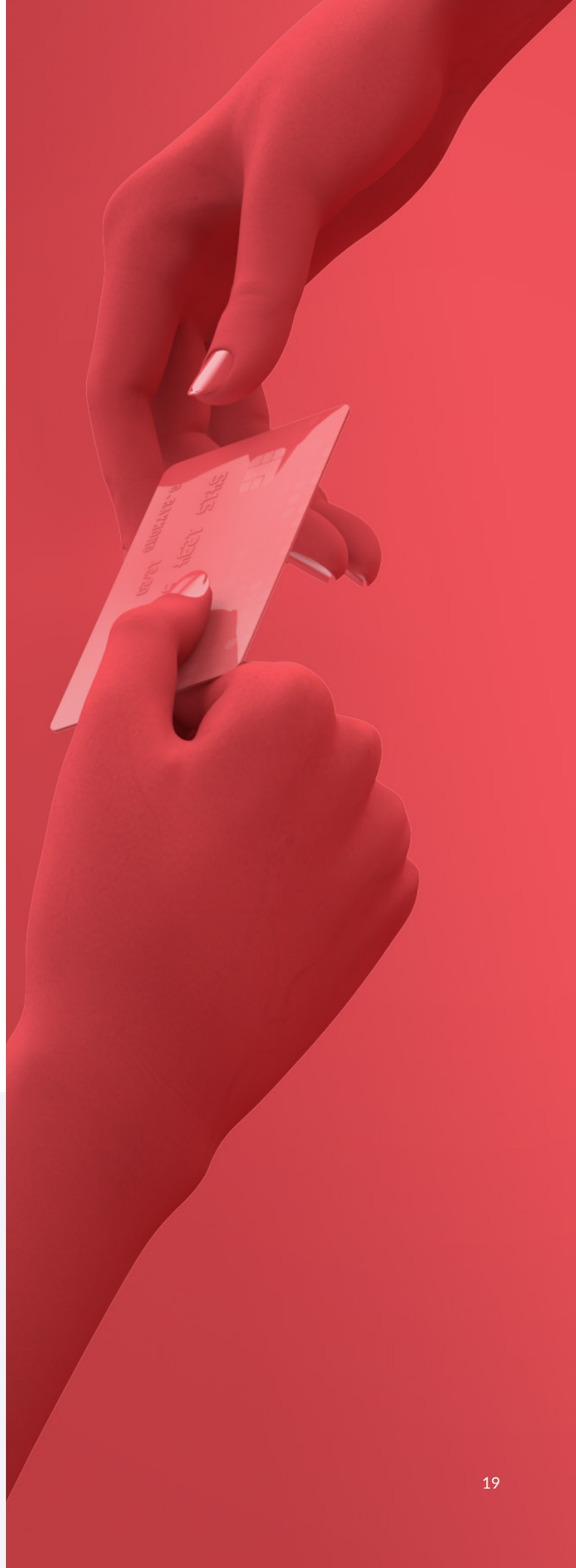
When processing transactions, there is a risk that the customer might dispute the amount charged. This is referred to as a *chargeback*, and when this happens, it's usually the business that is responsible for refunding the money to the customer. But what if the business is unable to provide the refund? In this case, it's the payment processor who is now responsible for refunding the money. The chance that a business may become insolvent or unable to meet their financial obligations is the risk that payment processors take in offering their service.

How to Sign Up and Why Underwriting Applies to Credit Card Processing

Much like a loan approval, processors look at several factors before approving a new merchant account.

THESE FACTORS INCLUDE:

- ✓ The specific industry your business is in
- ✓ The volume of credit card purchases
- ✓ The average size of transactions
- ✓ The delay between customer purchase and product received
- ✓ Financial Health of the Merchant





Personal credit checks or business financial statements are often required when you're signing up for a new merchant account to ensure that the business and its owners are able to financially support any chargebacks or refunds that might occur.

When you sign up for an account you may be asked for this information, so the payment processor can evaluate the level of risk that allowing you to accept payments will expose their business to. There are some businesses that do not fall easily into a category of risk that would be deemed acceptable by most processors, and for those businesses, they may need to enlist the services of a high-risk payment processor.

Once the payment processor receives your business's information, they will review the documents and if anything is missing then they will typically reach out to let you know. Once all the required documents have been submitted, they will be sent to the underwriting department. Once underwriting has completed their review of your documents, your account can be approved.

All processors usually employ similar underwriting requirements and reviews to manage their risk when accepting new businesses. We cover the financial risks of accepting and processing credit cards in a later section of this guide.

Processor Types

When shopping for a payment processor, there are several different types of processors that you can choose to sign up with. Although they are all offering payment processing, there are pros and cons that we will highlight in the section below. Different processors will be better suited for some industries and businesses over others, so it's worth doing your research to see which provider is best for your business. Ultimately, all providers will let you accept credit cards, but understanding how they're structured and who they might be partnering with to deliver their services can help you make an informed decision.

The Bank Processors

The large, bank-owned processors in the United States are First Data (now Fiserv), Chase Paymentech, Elavon, Global Payments, Vantiv, and Wells Fargo. In Canada, they are TD Merchant Services, Moneris, Desjardin, and People's Trust.

The way you feel about a bank processor will most likely be like how you feel about your bank as a day to day consumer. Do you feel like your bank provides you with the lowest rates, the best customer service, and the most cutting-edge software and services in the industry? Probably not,

though you can likely count on them for securely storing your money and treating you with respect.

With the bank processors, status-quo is the name of the game. They have millions of merchant locations and decades of established business history, so these providers rarely need to innovate their services or payment tools. Instead, they focus on maintaining their margins and market share through their well-established distribution channels. Bank processors may be slower to add new technology to their offerings, which may be limiting for some businesses who are looking for new integration options or who are looking to keep up with the evolving demands of their customers.

It's important to note that these providers are also the backend partner for nearly all the processors listed below, even the new wave of Silicon Valley payment providers, and for Helcim as well. If you read the fine print in any merchant account agreement, one of the bank processors will be listed as the backend acquirer. In a way, this means that they are unavoidable as they hold the keys to accessing the Visa and Mastercard networks. However, adding the right (or wrong) partner in between your business and the bank processor can make a world of difference.

A Quick Note on Review Websites

Many merchants try to learn about their payment processor alternatives through review websites, however, not all review websites are created equally. Most review websites (especially in the financial services spaces) are operated by for-profit companies, who may be incentivized to promote service providers with high-reward affiliate and referral programs, over those with the best rates or service. Unfortunately, this can create a conflict of interest with unsuspecting merchants, who think they are reading unbiased reviews online.

MSPs and ISOs (Resellers)

Merchant Service Providers (MSPs) and *Independent Sales Organizations* (ISOs) essentially resell a payment processor's product and use them for transaction processing. They are commonly referred to as resellers, and the pricing and service you might receive from them can vary from being fair to downright dishonest.

While resellers might be willing to offer you lower processing fees than you would be able to get by signing up with a processor directly, they are just as likely to charge higher rates, include extra or hidden fees, or have long-term contracts that are difficult to cancel in order to make up their own margins. As with any other payment processor that you might be considering, it's important to carefully review the processing fees, contract terms, and any applicable charges that might be applied to your account. While some resellers may offer better customer service because they are a smaller company with fewer merchants, others may offer poorer customer service and simply blame the processor for issues you encounter without providing a solution.

If you're considering signing up with an MSP or an ISO, then it's important to do your research into the specific company you're considering. Reference a variety of online reviews on different websites, check for reviews on [Google](#), [Facebook](#) or other similar sites, and check the [Better Business Bureau](#) to get a sense of what experiences other merchants have had with them.





High-Risk Payment Processors

Sometimes a business might be deemed *high-risk* if they operate in one of several flagged industries or if there are concerns about financial stability about either the business or the business owners. Generally, any business involved in selling weapons, adult materials, drugs or drug paraphernalia, or other higher-risk products can expect to be met with added scrutiny and may not be approved by some processors.

There are, however, certain high-risk processors that specialize in approving and providing payment services to high risk businesses, usually at the cost of significantly higher processing fees, increased document submission requirements, and lengthy fund holds called reserves.

Retailers Selling Merchant Services

It can seem strange that you can sign up for a merchant account while also stocking up on a family sized bag of snacks and a massive pack of your favorite soft drink, but if you've browsed through your local retail warehouse club, you might have noticed that they may also offer merchants services. The retail warehouses are essentially resellers offering merchant services on behalf of their backend processor. While they might offer great discounts on snacks and drinks, the lower pricing may not extend to their merchant accounts. In addition to their processing fees, you likely need to maintain a membership with the retail warehouse club to sign up for their merchant services.

A Quick Note on Associations, Chambers and Lobby Groups

If you're a member of a local Chamber of Commerce, professional association, or business lobbying group, then you might have noticed that they have a recommended processor under the "Membership Benefits" section of their website.

Members may assume that this processor was carefully chosen as the most affordable and best-fitted choice for its members and that their association would not be profiting from their choice. Unfortunately, this assumption isn't always necessarily correct as there is often an arrangement in place that directly benefits the chamber or association, and it's still a good idea to do your own research.



The Payment Facilitators

Payment Facilitators, or PayFacs for short, are a relatively new type of payment provider, but they've had a significant impact on the industry in recent years. Helcim is a PayFac, along with Square, Stripe, and PayPal who are all household names because they've changed the way people think about payments.

These providers are issued one master Merchant ID, or MID. It is under this single master MID that they are essentially able to aggregate all

their merchants as sub-merchants (the old terminology for these providers was “aggregators” for this very reason). Since the PayFac itself takes on the risk of underwriting all their merchants, they are able to offer their merchant services in a very streamlined manner, while often expediting their onboarding process. Some PayFacs may opt to offer flat-rate pricing, which can cost more, to compensate for the risk they are taking on by not requiring as much application information from the merchant.

The Software Platform

There are now more software companies who also offer integrated payments than ever before because of the influx of payment providers coming out of Silicon Valley. Generally, the primary focus for software platforms is online transactions, which is something to keep in mind, especially if your business needs card-present solutions. Some of the most well-known examples of software platforms that offer payments as part of their service are FreshBooks, Salesforce and Shopify.

One thing to note is that software platforms offering integrated payment solutions are essentially just resellers of their partner processor, and for this reason, they usually cannot offer the lowest rates. This is because in order for them to benefit from the processing, they need to add an additional margin on top of their existing partner processor's margin. So, while you may have the added functionality of the software, many merchants soon realize that the cost of their processing can quickly eclipse the cost of the software's monthly fee.

VICTORIA AVENUE
HOPE, BC, H3L 2J3 , CAN

DEBIT CARD STATEMENT

SERVICE PLEASE CALL
MEMBER, 4357891HN0006 800-210-5678

AMOUNTS FEE/CHRG CAT.
8,850.00 CREDIT CARD
0.00 EBT
0.00 PIN DEBIT
0.00 AMERICAN EXPRESS
0.00 OTHER EXPRESS
0.00 MONEY TXN
0.00 CARD MANAGER
0.00 DEBIT MIN BILL
0.00 ELEC CHECK BILL
0.00 CARD MIN BILL
0.00 WITH ASSOC FEE
0.00 OTHER FEES
0.00 CHRG/FEE

FEES SUMMARY
22.92
0.00
0.00
0.00
0.00
0.00
0.00
0.00
0.00
0.00
1.57
6.11
174.56
205.16

340.00
1.72

1,140.00
1.71

370.00
0.07

FEES, AND

00012
AMOUNT

3

1

FEES RATES & PRICING

There are several different pricing models that payment processors might offer and we will review them in more detail in the section to follow. The pricing structure that is best for your business will depend on a few different factors, but most importantly, how much your business is processing each month, which is referred to as *processing volume*.

In addition to the payment processing fees you will be charged, there are several additional per occurrence fees that you may need to pay. It's important to understand what fees you are being charged in order to get a full and complete picture of your monthly statement and what your processor is charging you and why.

▶ What is the Interchange Rate?

The *interchange* fee is the fee that is set and collected by the card brand for accepting the particular credit card. Each type of card transaction has a base fee that is charged to the merchant by the cardholder's bank.

Interchange isn't just one, constant rate, there are actually hundreds of varying rates that could apply to a given transaction based on several different factors such as the type of credit card the customer uses, how the transaction is processed (card-present versus card-not-present or online), and what kind of business you are. These factors will impact which rate you are charged by the card networks.

For example, swiping a credit card or using the chip will result in a lower rate than if you were to manually enter the card information on a website, this is because there is more inherent risk in the latter situation. The type of business you run and the industry it operates in can also affect the rate. For example, charities are eligible for lower interchange rates than restaurants are. Finally, customers get to choose from a wide variety of

different types of credit cards, and transactions involving a basic cash back card will have a lower interchange rate than transactions processed with privilege or travel rewards cards.

When Does the Interchange Fee Apply?

The interchange fee will apply each time you process a credit card transaction. The fee that the processor will charge your business includes an interchange fee, a card brand fee, and their own margin in each transaction that you process.

Where Can I Find a List of Interchange Rates?

Visa, Mastercard, and most other card brands are now required make their interchange rates public. You can find breakdowns of interchange rates on our website at the links below.

LIST OF INTERCHANGE LINKS

[Canadian Visa Interchange Rates](#)

[Canadian Mastercard Interchange Rates](#)

[Canadian AMEX OptBlue Rates](#)

[Canadian Discover and China Union Pay Interchange Rates](#)

[USA Visa Interchange Rates](#)

[USA Mastercard Interchange Rates](#)

[USA AMEX OptBlue Rates](#)

[USA Discover and China Union Pay Interchange Rates](#)

Why Do I Need to Know What It Is?

Understanding the interchange rate, how it is applied, and how it can vary from transaction to transaction can help you make sense of your processing statement each month, especially if your processor uses Interchange plus pricing. Knowing more about the payment processing industry in general can help in understanding the service that processors are offering and, if need be, advocating for your business.

What Are Payment Processing Rates Made Up Of?

Let's take a common processing flat-rate of 2.9% + 30 cents. This fee, that is charged for processing a payment, is made up of three smaller fees that are combined to make up the final fee charged by your processor. These parts are:

Fee 1: Interchange Fee – The base fee to process the transaction. This fee changes depending on the type of credit card that was used by the consumer, your business's industry, and how you are processing the transaction (in-person, keyed, online). For this example, let's say the Interchange amounts to 1.70% + 10 cents.

Fee 2: Card Brand Fee – A small fee that the card brand (Visa, Mastercard, AMEX, Discover) takes for each transaction. For example, a traditional Visa credit card that is used for a swipe transaction in the US has a 2.2¢ + 0.140 % card brand fee associated with the transaction.

Fee 3: Payment Processor Margin – The fee the payment processor takes for providing you with the ability to take payments and for the associated risk of underwriting merchant accounts. For this pricing example, the processor's margin would be 1.06% + 17.8 cents

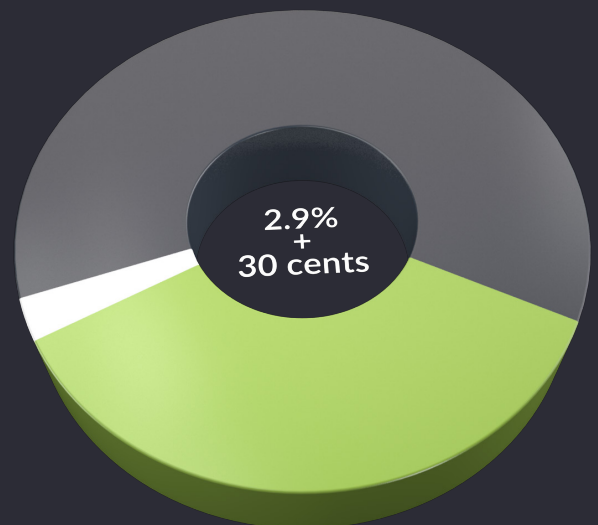
Lets use a transaction amount of \$100 for this example:

Interchange Fee:
 $1.7\% + \$0.10 \text{ cents} = \1.80

Card Brand Fee:
 $0.14\% + \$0.022 = \0.162

Payment Processor Margin:
 $1.06\% + \$0.178 = \1.238

Total cost:
 $\$1.80 + \$0.162 + \$1.238 = \3.20



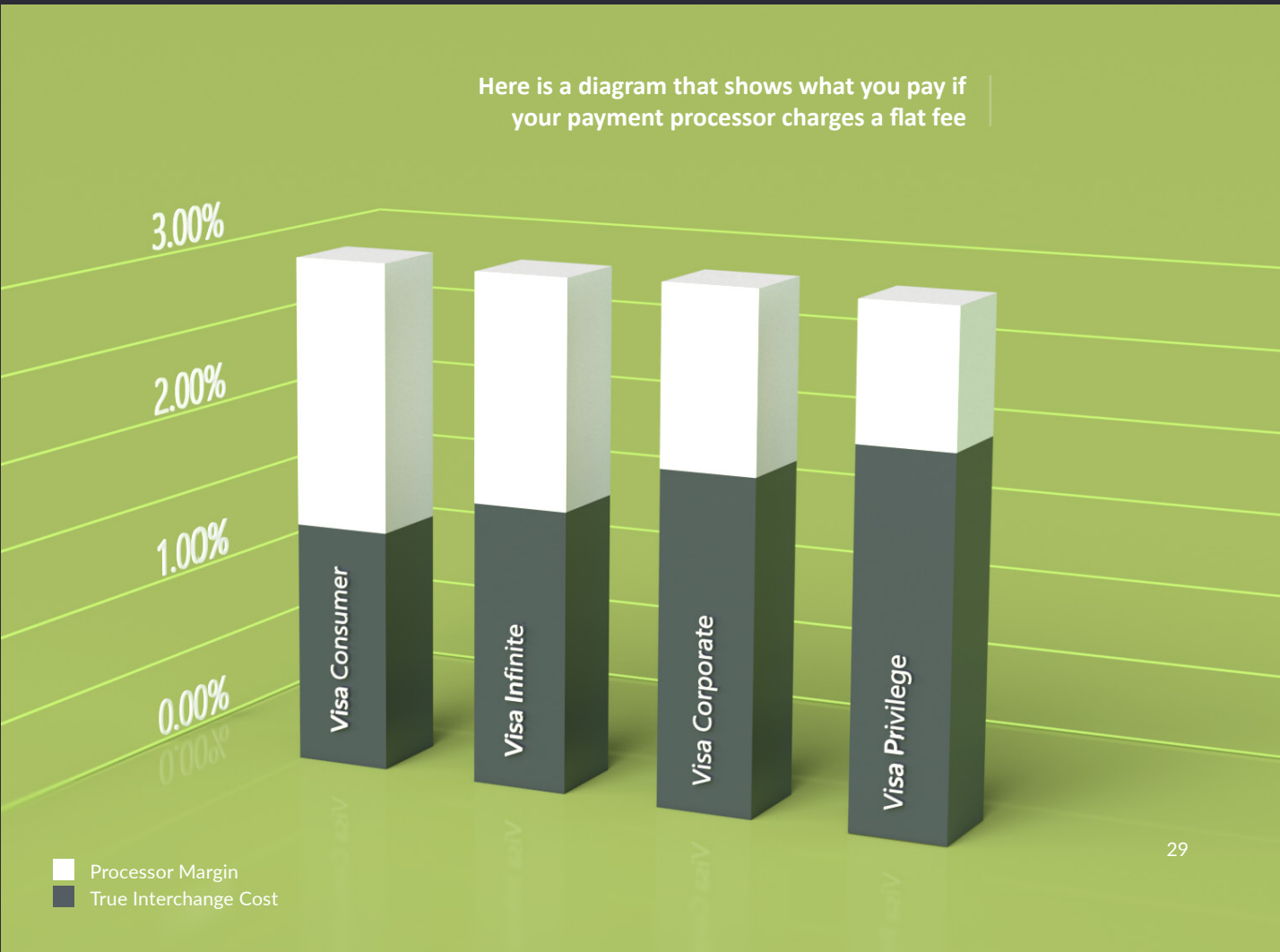
Types of Processing Pricing

Flat Rate Pricing

If your payment processor offers a *flat rate pricing* structure, then they have taken the interchange fee, the card brand fee, and their margin fee to determine one single rate that will be applied to all the transactions that your business processes.

Because this is a flat pricing structure, you pay a single rate, like 2.9%, on *all* of your transactions, even if the actual interchange rate varies with the different transactions. Depending on your business and the volume you are processing each month, this may mean that your business is paying more than it needs to for payment processing.

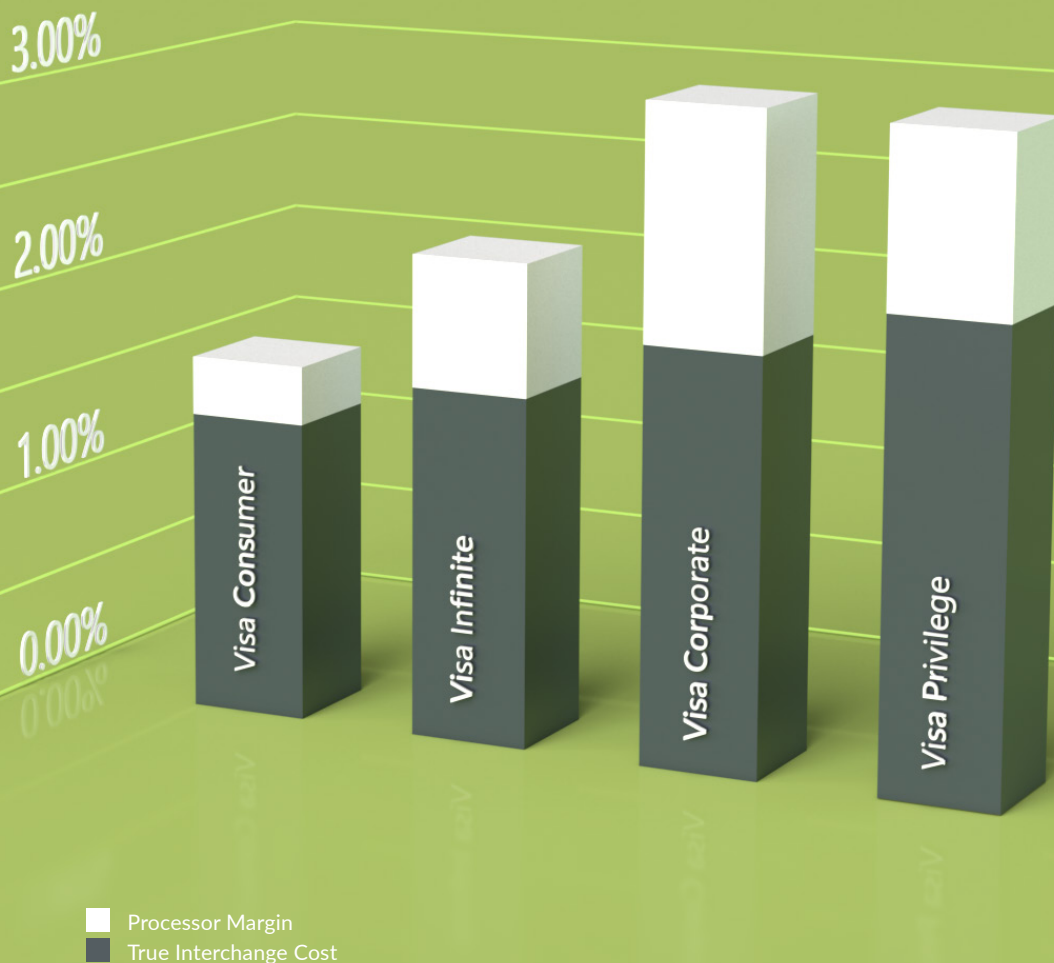
Many merchants are lured by the simple nature of flat rate pricing and only having to be aware of a single fee for all transactions, but may eventually realize their business has outgrown this model or could have been saving money with another processor all along. So, while this pricing model may seem simple or easier to understand, it's important to compare it with other processors' models to ensure you are, in fact, getting the best deal possible for your business.



Tiered Pricing

Tiered pricing usually consists of having a lower "qualified" rate for certain transactions and higher "mid" and "non-qualified" rates for others. This is the most common pricing method in the US. The common drawback is that merchants are enticed with a low "qualified" rate, which usually only applies to very select few types of cards, but nearly all transactions end up in the higher "mid" and "non-qualified" tiers.

Here is a diagram that shows what you pay if your payment processor charges tiered pricing

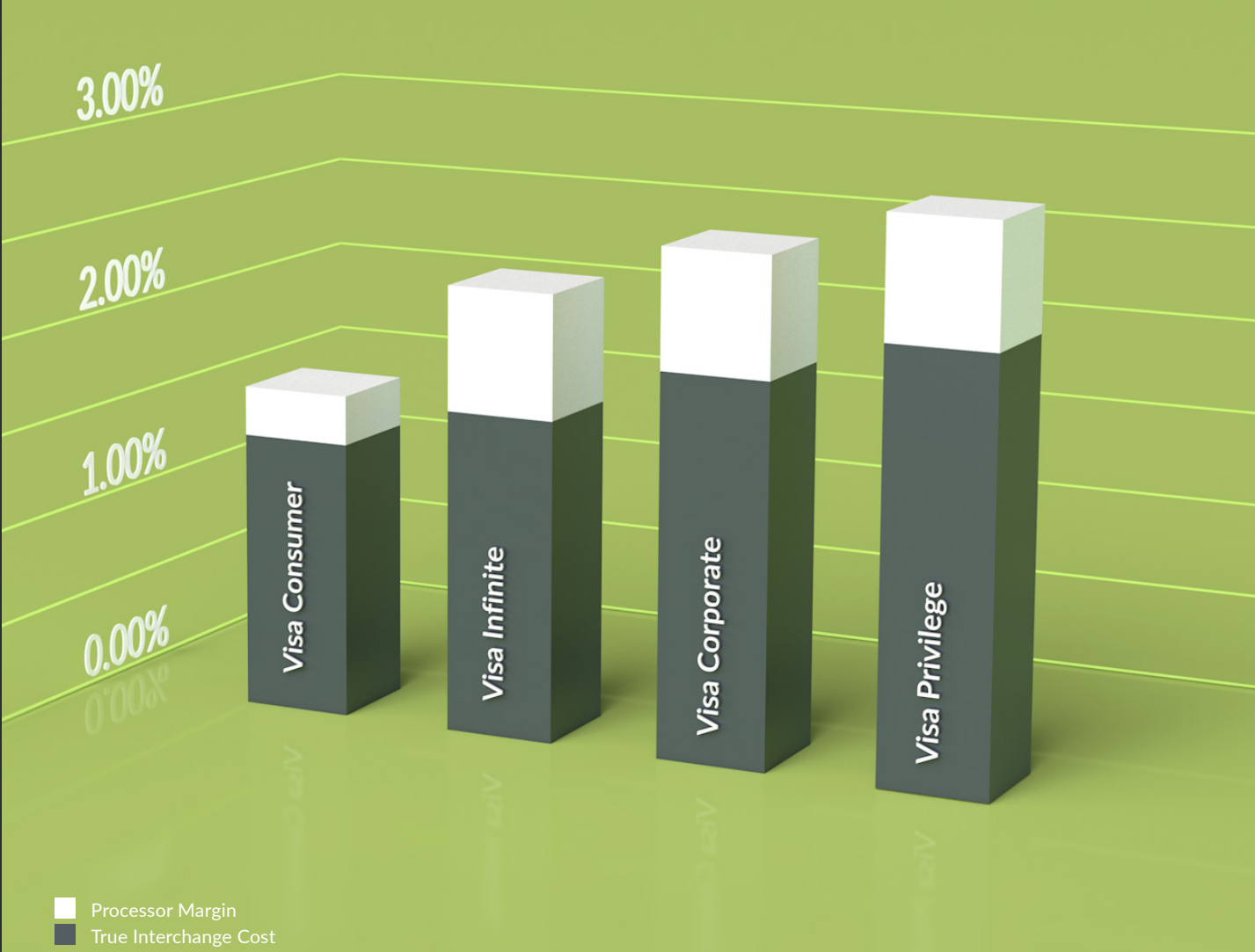


Differential Pricing

While less common in the US, *Interchange Differential* is more common for Canadian processors.

Similar to tiered pricing, "qualified" and "non-qualified" fees are charged, but merchants are also charged *interchange differential fees* for credit cards. This results in merchants paying multiple fees on the same transaction, essentially being double billed.

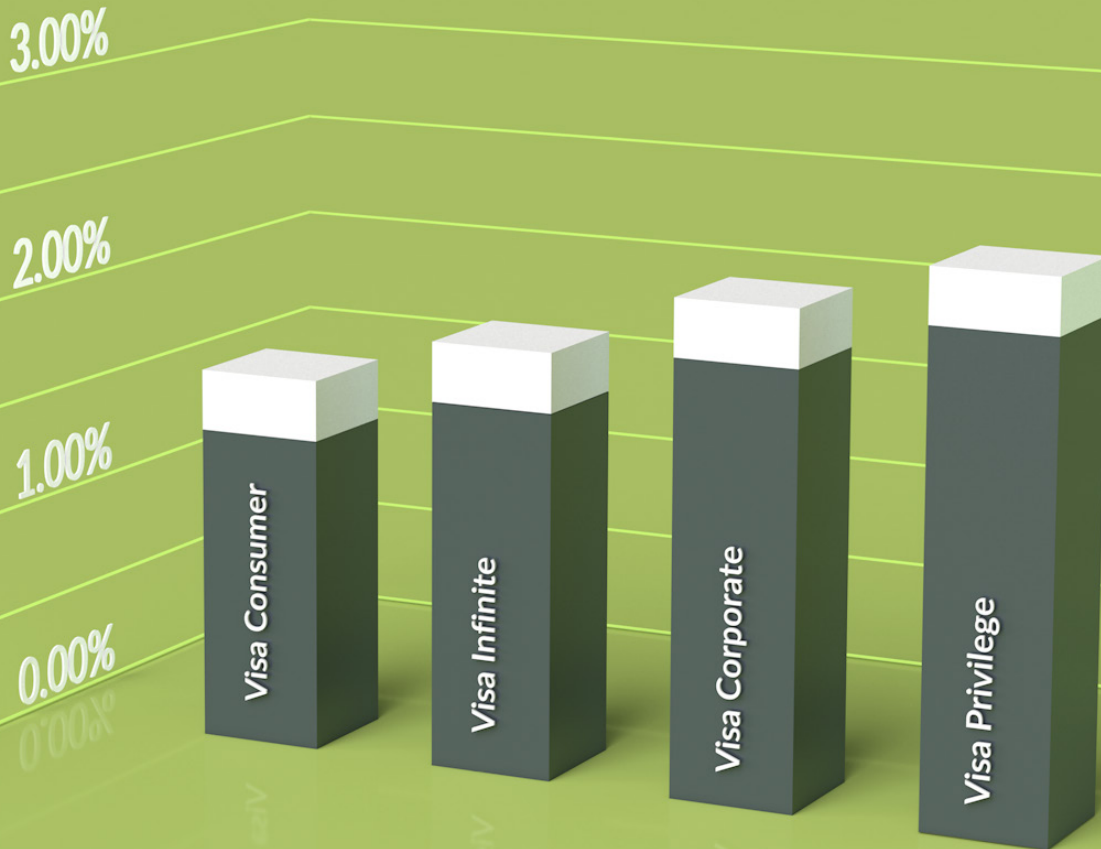
Here is a diagram that shows what you pay if your payment processor charges differential pricing



▶ Interchange Plus

Often considered the most honest and affordable pricing model in the industry, *interchange plus* pricing creates a very transparent relationship between a merchant and their processor. With this pricing model, the processor margin will be a set percentage across all transactions, while the interchange fee, which fluctuates depending on which type of transaction is being processed, will dictate the final cost of a given transaction. This means that whenever you process a transaction that is eligible for a lower interchange fee, you will save money compared to if the transaction was completed using a straight flat rate for all transactions.

While Interchange Plus pricing may seem more complicated to begin with because of the many different interchange rates out there, it can result in significant savings for your business.



■ Processor Margin
■ True Interchange Cost

Understanding Additional Fees Related to Credit Card Processing

Outside of the processing rate, there are a number of per occurrence fees that might be charged by your payment processor. Understanding what each fee is can help you avoid bad processing agreements and unfair billing practices. With any of the fees listed below, there is the potential for excessive processor inflation and unjustified billing. It is up to you as a well-informed merchant to do your homework, ask the right questions, and get rate comparisons to ensure you're getting the best arrangement for your business.

Monthly Minimums

Many processors will charge a *monthly minimum* on top of their standard monthly fees. This monthly minimum is the minimum amount you must pay the processor in *processing fees alone*. This means that if you don't reach this minimum amount, you'll be charged a difference by your provider as a penalty. Some processors will blame Visa or Mastercard for these minimums, but these fees have nothing to do with Visa or Mastercard and are instead pocketed by the processor charging them.

Statement Fee & Admin Fees

Many processors will charge additional *statement fees* or *admin fees* on top of their standard monthly fee. It can be a good idea to ask why they are charged or what they actually cover.

Quarterly Fees & PCI Fees

Many processors have recently started charging *quarterly fees* or monthly *PCI fees*. Sometimes processors will roll their legitimate cost of keeping a merchant PCI-compliant into their monthly fee, or even into a percentage of transactions fees. Some processors will grossly inflate this fee, in some cases up to 1% of the total transaction, in order to profit off the merchant.

PCI Non-Compliance

If your business is following the data security standards set out in the Payment Card Industry Data Security Standard (PCI DSS), then you would be considered PCI Compliant. The requirements for compliance will vary based on your business, but if your business does not meet the PCI DSS requirements, then a *PCI non-compliance fee* could apply in order to incentivize compliance going forward.

Setup & Application Fees

Many processors will have a *setup fee* for your merchant account. Some will even charge a separate *application fee*, which is non-refundable even if your merchant account application is declined.

Early-Termination, Contract Closure & Leasing Fees

Many processors have a 3-5-year processing contract, with *cancelation fees* ranging from \$250 to \$5,000 or more. Merchants who sign equipment lease agreements can also face large equipment buyout rates. We'll talk about why you should avoid terminal leases at all costs later.



Monthly Fee

A *monthly fee* typically covers some of the costs the processor needs to pay to be able to provide payment processing to the merchant and shouldn't necessarily be considered a non-starter. What this fee includes will vary depending on your payment processor and it's worth asking what it covers, and what it doesn't, before you sign your merchant contract.

Processors that do not have a monthly fee often have these costs built into their margin which usually results in higher processing fees. This is why processing volume is so important because if you are processing above a certain amount per month, a monthly fee can often be absorbed by the savings your processing volume affords you.

International Cross-Border Fees

Visa and Mastercard charge a *cross-border fee* if the customer is outside of your business's home country to help manage currency exchange costs. This fee varies depending on your processing currency.

Bank Account Change / Business Name Change

This per-occurrence fee may apply in the event that you decide to change the business name that appears on your customer's credit card statements, or if you decide to change the bank account that receives your processed funds.



NSF Fee

Processing fees for the processed funds are generally removed from your bank account at the end of each month, as well as any applicable fees (such as the monthly fee). It is your responsibility to keep an appropriate balance in your bank account for these fees. In the event that these fees cannot be debited, an *NSF fee* will apply, and another withdrawal may be attempted within the same month. If these additional withdrawals fail, you will be notified of the overdue account. Merchants with an overdue account risk having their account closed.

Chargeback Fee

In the event that a customer files a complaint with their issuing bank against a transaction you processed, you will be notified and given a 30-day window to dispute the complaint. A *chargeback fee* will be levied against you for the occurrence. If you ultimately win the dispute, some processors will reimburse the chargeback fee, but most will not.

Voice Authorization Fee

In the event that a cardholder's bank requires further information to authorize a transaction, the terminal or virtual terminal may display the message "CALL AUTH CENTER," giving you the option to call the voice authorization center and obtain approval code. In such a case, a *voice authorization fee* will be applied.

EQUIPMENT & SOFTWARE



Different processors will offer a variety of different equipment and software options, allowing you to facilitate transactions with the card present, or online. Before you sign a contract, ensure they have the tools that your business will need to accept payments however and wherever you need to. In addition to how you want to accept payments, take note of any software integrations or requirements that would help your business, and confirm with your selected payment processor that they will be able to provide the functionality you're expecting.

helcim

Solutions for Card-Present Transactions

As payment methods and hardware technology continue to evolve, new payment devices continue to be introduced to the marketplace to allow you to accept payments in person. Each piece of hardware is unique and will vary on which payment methods they support. These methods include magstripe swipe, Chip, Chip & PIN, and tap (NFC). Their available connectivity also varies, such as ethernet, Wi-Fi, Bluetooth, audio jack, 3G, among others. Merchants are not short on hardware options, and each component needs to be carefully selected based on your business needs.





Credit and Debit Terminals

If you are accepting payments in person, then you will need to decide which *terminal* is right for your business. There are a variety of wired and wireless terminals available to choose from that will allow you to quickly and easily accept payments in person.

What makes a terminal different from mobile readers is that they don't need to be connected to a computer or paired with a device (such as a

phone or tablet). These terminals can operate in a stand-alone environment as long as they have internet or phone-line connectivity. This means that a merchant can easily add a terminal to their store's countertop and simply accept payments. The frequent downside of terminals is their lack of software and functionality, they typically only offer basic payment functionality and lack any "smarts" or data-driven insights that a true Point-of-Sale system would provide.

Card Readers

Card readers, unlike terminals, typically rely on another device that they need to pair with for connectivity and to be able to initialize transactions. These devices can include phones, tablets, Macs, PCs, and other workstations. While this dependency may be seen as a disadvantage, there are also numerous benefits to using a card reader.



MOBILITY

By pairing with phones and using their data, card readers allow for easy on-the-go payment acceptance.



LOWER COST

Since they are dependant on another device to provide some of their functionality, card reader hardware is relatively simple compared to other hardware options meaning it can often be priced lower than terminals. There is also the added savings of not having to outfit your long-range terminal with a SIM card and paying monthly for separate data.



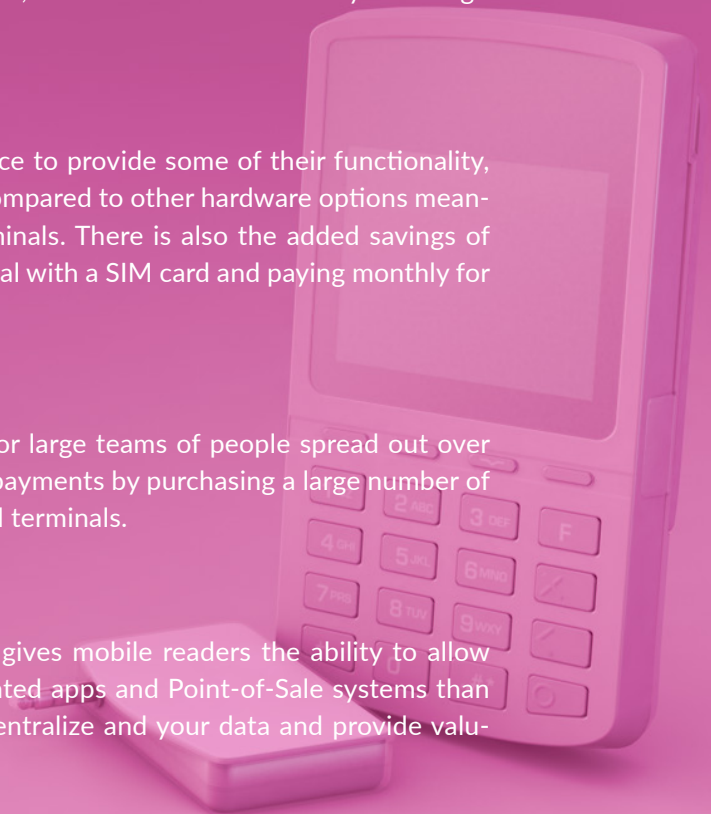
SCALABILITY

Merchants that have numerous locations or large teams of people spread out over multiple locations often choose to accept payments by purchasing a large number of card readers at a lower cost than individual terminals.



SMART DATA

Pairing with smartphones and computers gives mobile readers the ability to allow payments to flow through more sophisticated apps and Point-of-Sale systems than typical stand-alone terminals which can centralize and your data and provide valuable sales insights.



The original card readers had limited connectivity options and were only able to connect with mobile phone audio jacks and only able to accept magstripe transactions. However, new card readers continue to be introduced with more connectivity and payment method options, blurring the lines between readers and terminals and redefining merchants' hardware requirements.

In Store Point-of-Sale System

If you are interacting directly with customers, then you will most likely need a *Point-of-Sale (POS)* system for your business. The traditional POS option is the standard cash register that you grew up with, however, new technologies in software and data collection mean that business owners have a wide variety of modern options to choose from today. Cloud-based POS software has made POS systems accessible for small businesses and they are able to completely replace the functionality of a cash register while increasing efficiency, lowering costs, and saving space. To use a mobile POS, you just need to download the application on your mobile device, tablet, or desktop and you can begin processing immediately.

Understanding Chip Cards

While on the topic of credit card readers and terminals, let's take a quick look at *chip cards*, or *EMV-enabled cards*.

EMV stands for EuroPay Mastercard Visa, after the three original companies that developed the standard. EMV was introduced in Europe in 2006, in Canada in 2010, and in the US in 2015. Interac Debit, which applies to Canadian merchants only, also changed over to the EMV standard in 2010.

EMV is often referred to as Chip & Pin because the most common way to use an EMV-enabled card is to insert the chip and then enter your personal PIN code. However, this is an oversimplification of the EMV standard, which also encompasses other transaction modes such as "Chip & Signature," where customers enter a card into a terminal and then sign instead of adding a PIN, as well as "Tap & Pay," where customers *tap* a chip card or phone against the terminal to pay.





Using EMV to Reduce Liability

While EMV has not completely replaced swipe for credit card transactions, if you choose to swipe credit cards instead of using EMV-enabled hardware, due to the recent liability shift, you are exposing your business to the risk of fraudulent transactions.

Card-Present vs. Keyed

To accept an EMV transaction all you need to do is use a terminal machine that supports EMV chip card transactions. When customers are ready to pay for their purchases, they simply use an EMV chip-enabled card. If a customer does not have an EMV chip card, it is up to you if you'd like to accept their card – and potentially open yourself up to unnecessary risk – or ask for an alternate form of payment.

EMV technology does not impact card-not-present (ecommerce or manually keyed) transactions as it only deals with card-present (retail) transactions. The requirements for manually keyed-in transactions have not changed, so they have not yet been impacted by EMV chip card technology.

▶ Near Field Communication

NFC (or Near-Field Communication) is a technology used in a multitude of contexts from product scanners and key fobs to file sharing and children's toys. If a credit card, debit card, smart phone, or wearable device is NFC-enabled, then they are able to pay for a purchase by simply holding their card or device close to the terminal, essentially facilitating contactless payments. Even though the card or device needs to be within about an inch and half of the terminal in order for the communication to occur, NFC payments are also commonly referred to as "Tap & Pay," "Tap & Go," or simply "Tap," because the user can simply *tap* their card or device on the terminal's surface to complete the transaction. Mobile and wearable payment technology, such as Apple Pay and Android Pay, also rely on NFC technology to complete transactions.



Solutions for Card-Not-Present (Online) Transactions

Virtual Terminal

A *virtual terminal* allows you to accept payments on your computer from anywhere, without the card being present. You simply log in to your workstation, laptop, tablet, or phone and authorize credit card transactions in real-time, all you need to complete the transaction is the credit card information from the cardholder.

Payment Pages

If you have an existing website that you need to add payment functionality to, then a *hosted payment page* might be the solution. Using a hosted payment page is an easy and secure way to accept payments online, save credit card information for recurring payments, and add a full shopping-cart checkout system to your website.

Gateway API

A *payment gateway* (sometimes referred to as a payment API or RESTful API) is a specific URL that has no user interface but is designed to receive an incoming transaction message. While most payment processors offer some type of payment gateway API built-into their service, some companies such as Authorize.NET and Cyber-Source are referred to as "payment gateway-only" service providers. This means that they offer their payment gateway service without a merchant account.

So why would you pay for a payment gateway-only service? Listed below are some instances that require it.

✓ **COMPATIBILITY**

The software or shopping cart you are using is not compatible with your processor's payment gateway but is compatible with a payment gateway-only service. This is a common usage of Authorize.NET, who is the most commonly integrated payment gateway.

✓ **MERCHANT ACCOUNT PROVIDER ONLY**

The provider does not have their own payment gateway. These merchant account providers will rely on reselling third-party payment gateways instead of developing their own payment gateway.

✓ **ADVANCED FEATURES**

The built-in payment gateway offered by your credit card processor does not have all the features you need. Some payment gateway-only service providers offer features such as card-tokenization and advanced fraud-protection that are beyond the scope of what most regular payment gateways offer.

The main downside of using a payment gateway-only service is that you would incur fees from both the credit card processor and the payment gateway company. However, for some, the benefits of the seamless payment integration warrant the additional costs.

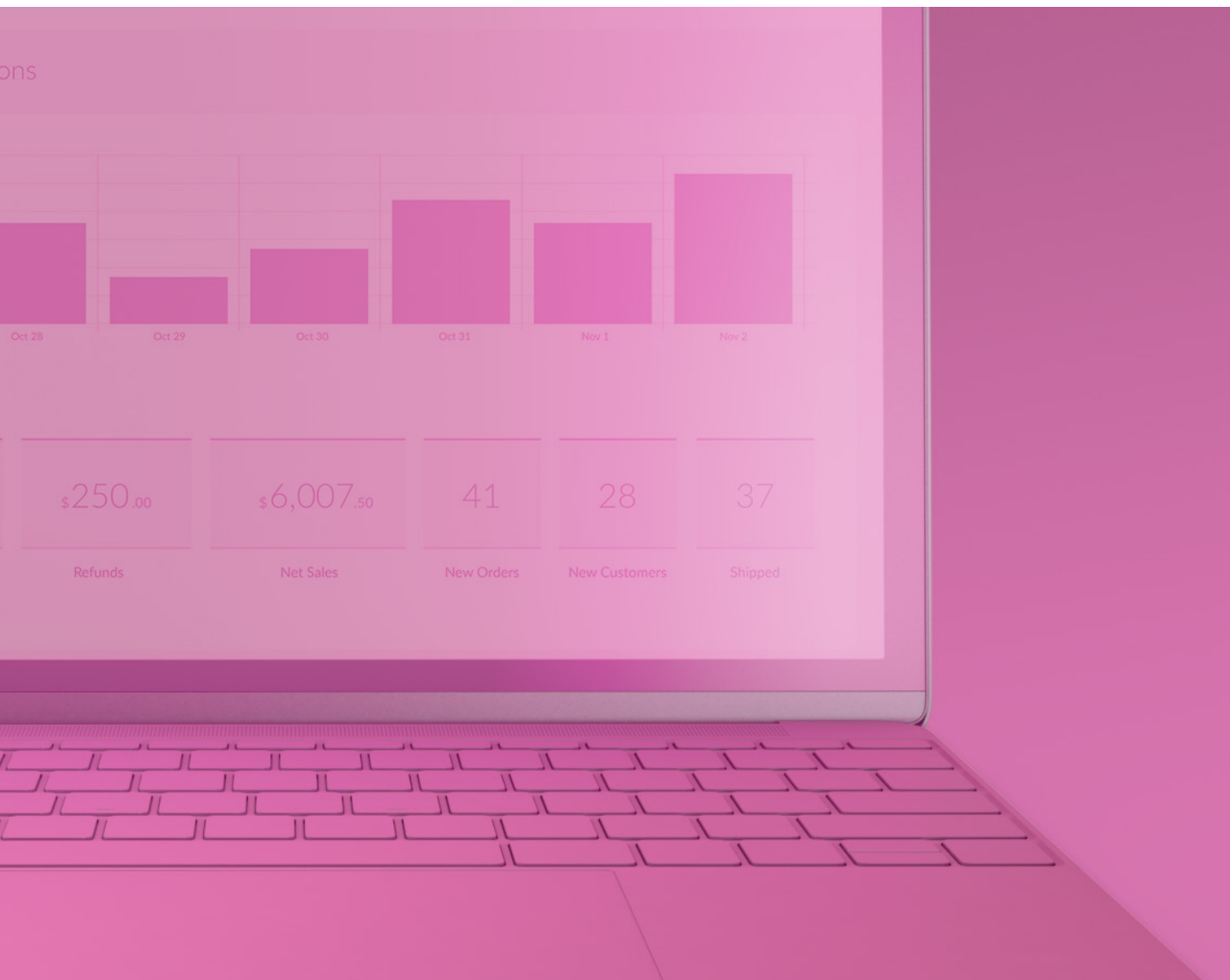
Because payment gateways work with your merchant account to allow you to process payments for customers, most credit card processors will provide both services to your business. While it is possible to find a payment gateway that only offers payment processing, most processors will offer additional services like payment notifications, checkout pages, subscription management, and credit card vaults. Having the same provider supply your merchant account and payment gateway along with all the additional functionality your business needs can simplify your business processes and make it easier to troubleshoot issues if they arise because it is the same company providing all the services.

Third-Party Software Integrations


Many payment processors include the ability to add *third-party shopping carts* and payments to the applications that your business is already using. Integration capability will vary by the processor so it's worth confirming which integrations they offer to confirm they can support the applications that your business is currently using.

Software

As the landscape of payment processing changes and evolves, so too do expectations for what a payment processor should provide. More and more, payment processors are packaging *business software tools* like invoicing, customer relationship management (CRM), recurring billing, inventory management, and others along with their offering, usually as paid value add-ons. Most processors partner with a software provider, but some develop their own proprietary software solutions to offer their merchants. It's worth asking your processor what kind of software they are offering along with their processing and if they charge for it.



PROCESSING PAYMENTS



You've selected a provider, signed up for a merchant account, and set up your equipment or software. Congratulations, you're now ready to start accepting credit cards! There's a lot more to accepting credit cards than just taking a payment, we outline all the different types of transactions and how it all works.

helcim

Card-Present vs Card-Not-Present

First, there are numerous ways to accept a credit card. They can be divided into two basic groups, *card-present* and *card-not-present*. As the name implies, a card-present transaction would include retail transactions where a customer completes the transaction in person, with their physical credit card. A card-not-present transaction would be any transaction where the card information is entered manually, either by the merchant or by the customer, like when a customer buys something online or has entered into a recurring billing cycle.

We will cover the pros and cons of each method in more detail below in the next section of this guide.

Regardless of which method is used to accept the card, the same types of transactions can be performed.

Card-Present

- ✓ It can be swiped using the magnetic stripe on the back of the card.
- ✓ It can be accepted using the chip (EMV) on the front of the card.

Card-Not-Present

- ✓ It can be manually entered into a virtual terminal, terminal, or website.
- ✓ It can be stored and used repeatedly in the future.



Transaction Types

Purchase

A credit card *purchase* (sometimes called a *sale*) is the most common and straightforward transaction type. Wanting to receive payment for a purchase from their customer, a merchant will process a credit card sale.

The credit card information (gathered by either card-present or card-not-present means) along with the amount of the sale is sent to the processor. The processor then sends all the transaction information to the card network, which then asks the customer's issuing bank to approve the transaction and requested amount. If approved, an approval code is returned to the merchant from the processor. This is achieved in real-time, meaning that within a few seconds, the transaction was processed and approved by the card network.

Pre-Authorization

A *pre-authorization* (sometimes called a *pre-auth* or just *authorization*) is very similar to a purchase, but it does not complete the sale. Just like a purchase, the transaction is processed in real-time, and an approval code is provided to the merchant for the desired amount. However, the funds are not debited from the cardholder, but instead "frozen" or "reserved" for between 7 to 10 days. When the merchant is ready to "capture" the pre-approved funds, the merchant will submit a *capture request* to complete the sale. This method is often used for hotels, car rentals, and gas stations, where the merchant needs to ensure that a certain amount is available on the

card, without charging the final amount until the service is complete or the charge is to be incurred. If a pre-authorization is not captured within seven days, the funds are unfrozen and released back to the cardholder.

Capture

Also known as a *force*, a *capture* is the second step after a credit card pre-authorization. For a capture to be successful, it must include the original approval code generated by the pre-authorization. Captures can be completed up to 30 days after the original pre-authorization, but funds are only frozen for the first 7 days. This means that while a capture transaction could be performed on the 20th day, there is no guarantee that the cardholder will still have the funds available on their credit card.

Captures can be up to the full pre-authorization amount or a lesser amount, but not for more than the original pre-authorization. For example, most gas station pumps do a pre-authorization for \$200, but the final capture amount (once you complete pumping your gas) is usually for a smaller amount. The uncaptured amount will be released back to the card.

Void

A *void* is used to cancel a previously authorized transaction. For example, if the incorrect amount was entered for a credit card purchase, the transaction can be voided and then processed again for the correct amount. A void transaction will be made in real-time to the card network, telling the customer's issuing bank to cancel the transaction and approval code. The customer will not be charged for the original transaction if it is voided. Voiding the transaction prevents interchange fees from being charged, but if it is processed as a refund, then you will not get the interchange fees back for that transaction.

A void can only be performed if the batch has not yet been settled (we'll talk more about batches later). If the batch has already been settled, a void can no longer be performed, and a refund would need to be performed instead.

Refund

Unlike a void, a *refund* can be performed after a batch has been settled. A refund is essentially a "negative" purchase, very similar to a stand-alone purchase transaction but with a negative amount instead of a positive. It is always recommended to void the transaction if possible, instead of performing a refund, because a voided transaction will not cause the customer to be charged for the original sale. If a refund is processed, the customer will see both the original charge as well as the refunded transaction.

The refund amount will be debited from the merchant (or from the most recent batch total) and sent back to the customer. While refunds are processed in real-time, the customer's issuing bank can take up to 10 business days to display it on the customer's statement.



Verify

A *verification* is a \$0 transaction. This is typically processed in a card-not-present scenario, where the merchant wants to verify the credit card but not actually process an amount at that time. Often, this transaction method is used to "tokenize" the credit card for later use. When you do a verification, you are checking the validity of the credit card number, expiry date, and card security. However, since no amount is sent, what is not being verified is the cardholder's available balance.

Approvals

When a transaction is *approved*, it is the customer's issuing bank, not the processor or the card network, that is approving the transaction. An approval means that the credit card number and expiry dates are valid, the customer has enough credit for the transaction amount requested, and that the card has not been reported as stolen or compromised. It is important to note that an approval is not an absolute guarantee of the transacted funds. There is always the chance a chargeback is filed at a later date by the cardholder, either because their card was stolen or because of a dispute with the merchant, which we'll get into in a later section.

Types of Credit Card Declines

Similar to how a transaction is approved, when a credit card is *declined*, it is declined by the issuing bank, as they are the entity that decides the outcome of the transaction, not the processor or the card network. Most issuing banks do not provide a detailed reason for the decline to avoid fraudsters from “testing” credit cards and trying to determine the reason for the decline. Card brands recommend that you do not try a card more than twice if you get a decline message, instead ask the customer for another form of payment. If you get a decline notice, there are a few primary reasons that are most likely the cause:

Declined - Invalid Card

When you receive an *Invalid Card* error, it means that the system has completed a MOD10 check, the checksum formula used to validate a variety of identification numbers, and the formula was unable to validate the card numbers, meaning the card you entered is invalid. This is usually because the credit card number was entered incorrectly.

Declined - Expired Card

If a customer has a card that has passed the expiry date listed on the front, then the card network won't be able to process it and they will need to present an alternate payment method or provide the updated expiry date.

Declined – ND

If you receive this message, then it is a normal decline by the bank. The most common reasons for a *Declined – ND* message are due to insufficient funds or a restriction placed on the card.

Declined - Call For Auth

This is also a decline, but there is a pathway for a potential approval. In this case, the bank is unsure about the transaction and would like the merchant to call the processor's call-for-auth center to do further verification on the transaction. If approved over the phone, the call center agent will provide you with an approval code for the capture.

Declined - Pick Up Card

This decline means that you should *actually pick up the card* if you are in the physical presence of it. Think of movies where the waiter takes scissors and cuts the card in front of the customer. This is because the card has been taken out of circulation, either because it was lost and has been replaced, or was reported stolen. While not a certainty, this can be a warning sign that a customer is trying to process a fraudulent transaction using a stolen card. It should be noted that a merchant should never compromise their safety in trying to repossess a credit card.

Tips for Dealing with Declines

Don't try processing the credit card multiple times. You will continue to receive decline messages, and your merchant account may be flagged for potential fraud or abuse. Instead, ask the customer for another payment method.

Try to avoid processing the credit card for a smaller amount – this may be seen as “testing” the card limit, and the transaction may be flagged for fraud. Instead of trying the transaction again, ask for another payment method from the customer.

For international transactions, some credit cards can have restrictions by default to decline all international payments. In this case, the customer

would need to call their issuing bank (the number can be found on the back of the card) and let them know they are trying to process an international transaction. The bank will “unlock” the card, and the merchant can try processing it again.

Some credit cards, especially business and corporate cards, can have restrictions on the type of purchases that can be made. Each merchant account has a SIC (standard industry code) associated with it, and a specific SIC could be prohibited from charging certain types of cards. In such an event, the cardholder again would need to contact their issuing bank to unlock the card before the merchant can try processing the transaction again.

What is CVV

The CVV on cards can go by a variety of names depending on which card brand issued the card, the different names are:

Visa: Card Verification Value (CVV)

American Express: Card Identification Code (CIC)

Mastercard: Card Verification Code (CVC)

Discover: Card Verification Data (CVD)

No matter what the company calls it, the CVV has one purpose, to verify that the cardholder has the physical card in their possession. Entering the wrong code will almost always result in the transaction being declined.

The CVV is not part of the data stored on the cards magnetic strip, or on the EMV chip, and as a business owner, you are strictly prohibited from storing the CVV information in your database or card vault. If a database was hacked and credit card numbers were stolen, the hackers would not have access to the security code, rendering the stolen information significantly less useful. The best practice for ecommerce websites is that they now require the CVV at checkout.

What is AVS

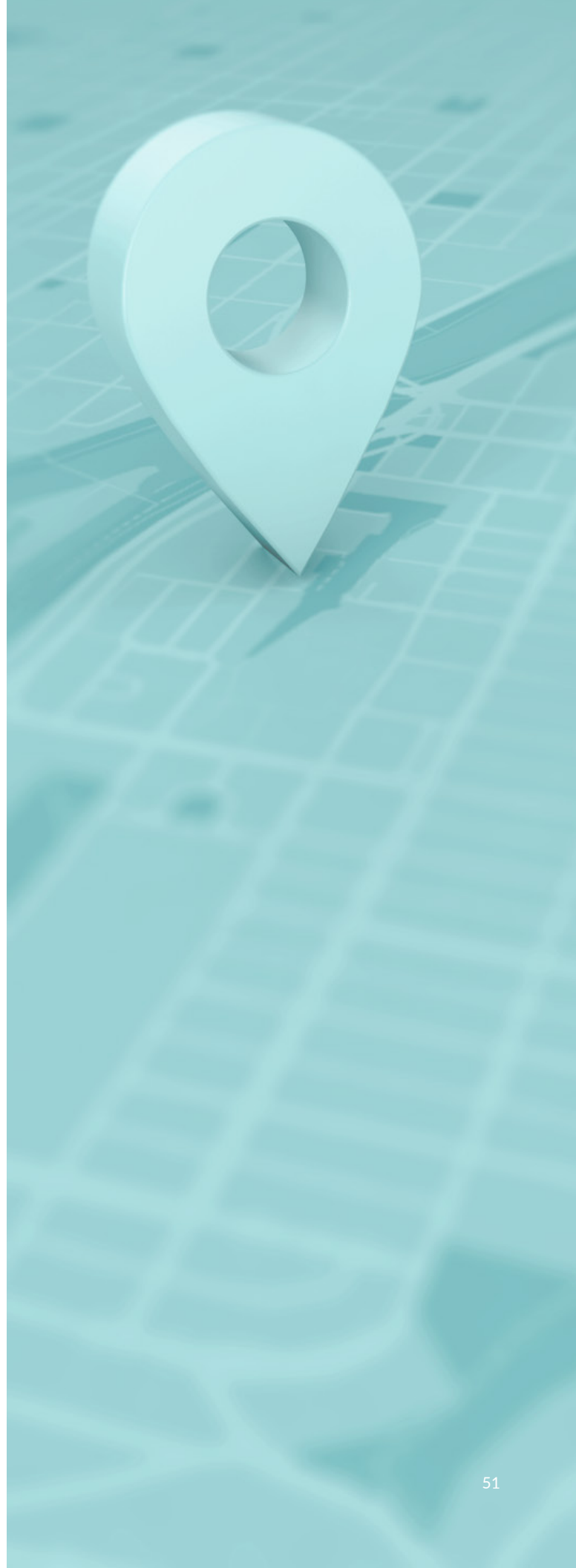
AVS stands for *Address Verification Service*. It's a tool that allows you, as a merchant, to check if the billing address of a credit card is linked to the address of the person claiming to own that credit card and making an online purchase. AVS is one of several fraud prevention tools that can prevent stolen credit cards from being used for online transactions.

When a customer has finished adding items to their shopping cart on your site and is ready to pay, they are brought to a payment form. On this form, they are asked to enter their credit card payment information, along with their billing address. This is also a common request when using a Virtual Terminal or [card vault](#).

While the credit card transaction is being processed, the system will also compare the billing address entered by the user at checkout with the address linked on file at the cardholder's issuing bank. As part of the transaction response, an AVS response code will be returned to you. The code you see could be "X" for "Exact Match," or "N" for "No Match," amongst others (see a full list of AVS response codes below).

It's important to note that the AVS result doesn't impact whether or not the transaction is approved or declined, it only gives you the result of the address match or mismatch. This means that if the customer enters an incorrect address, the transaction can still be approved by the bank. It will be up to you as the merchant to decide if you're comfortable going ahead with shipping the item to the customer, or if you want to cancel the order and refund the transaction.

AVS is one of many tools that you can use to review orders and prevent fraud. When you combine an AVS system with other security measures like requiring a CVV on your credit card transactions or implementing a fraud detection tool, you can reduce the risk of exposing your business to fraudulent orders.





AVS Response Codes

Response Code

Description

A	Address (Street) matches, ZIP does not
B	Street address match, postal code in wrong format. (international issuer)
C	Street address and postal code in wrong formats
D	Street address and postal code match (international issuer)
E	AVS error
F	Address does compare, and five-digit ZIP code does compare (UK only)
G	Card issued by a non-US issuer that does not participate in the AVS System
I	Address information not verified by international issuer
M	Street address and postal code match (international issuer)
N	No match on address (street) or ZIP
P	Postal codes match, street address not verified due to incompatible formats
R	Retry, system unavailable or timed out
S	Service not supported by issuer
U	Address information is unavailable (domestic issuer)
W	9-digit ZIP matches, address (street) does not
X	Exact AVS match
Y	Address (street) and 5-digit ZIP match
Z	5-digit ZIP matches, address (street) does not

Batches and Settlements

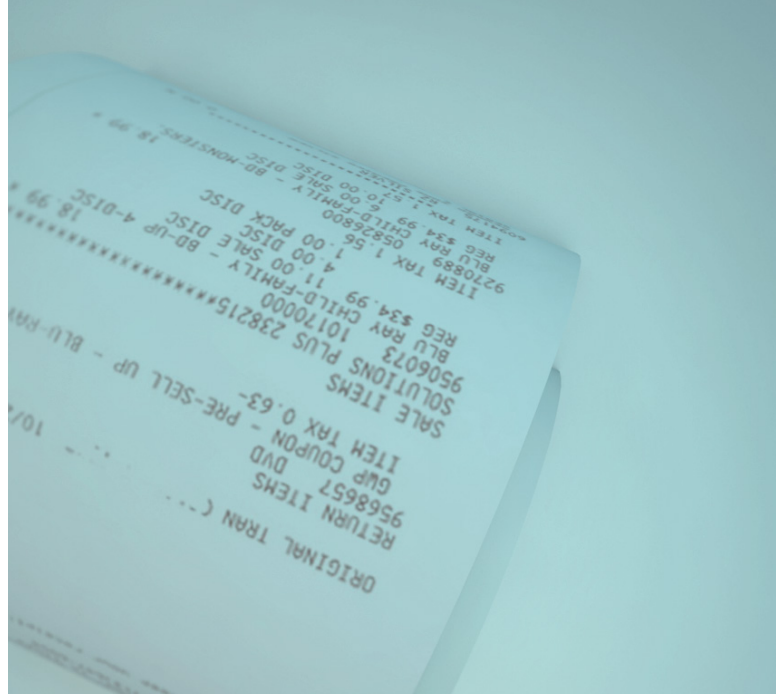
It's important to understand that while credit card transactions are processed in real-time – meaning that when a transaction says it has been approved, it has been approved by the cardholder's bank near instantly – receiving those funds to your bank account is not a real-time process. When a transaction is approved, it is added to your *batch*. A batch is a group of transactions that have been processed but have yet to be settled. When a batch hasn't been settled yet, it is called an open batch, and transactions in the batch can still be voided and reversed if needed. Once you're ready, you can close a batch and trigger a settlement. For most merchants, this is typically done automatically at a set time each day. However, some merchants, like retailers and restaurants, prefer to manually settle their batches during their end of day cash-out.

If batches are left open for too long (typically 48 hours to 6 days), some processors will choose to automatically close and settle the batch, while others will let the unsettled transactions expire. By leaving batches unsettled for too long you may also be exposing your business to the risk of transaction downgrades or lost transactions, so we recommend you regularly settle your batches yourself instead of leaving them open.

Here is an example of what a batch might look like:

1	Visa	\$100
2	Mastercard	\$50
3	Visa	\$75
4	Amex	\$150

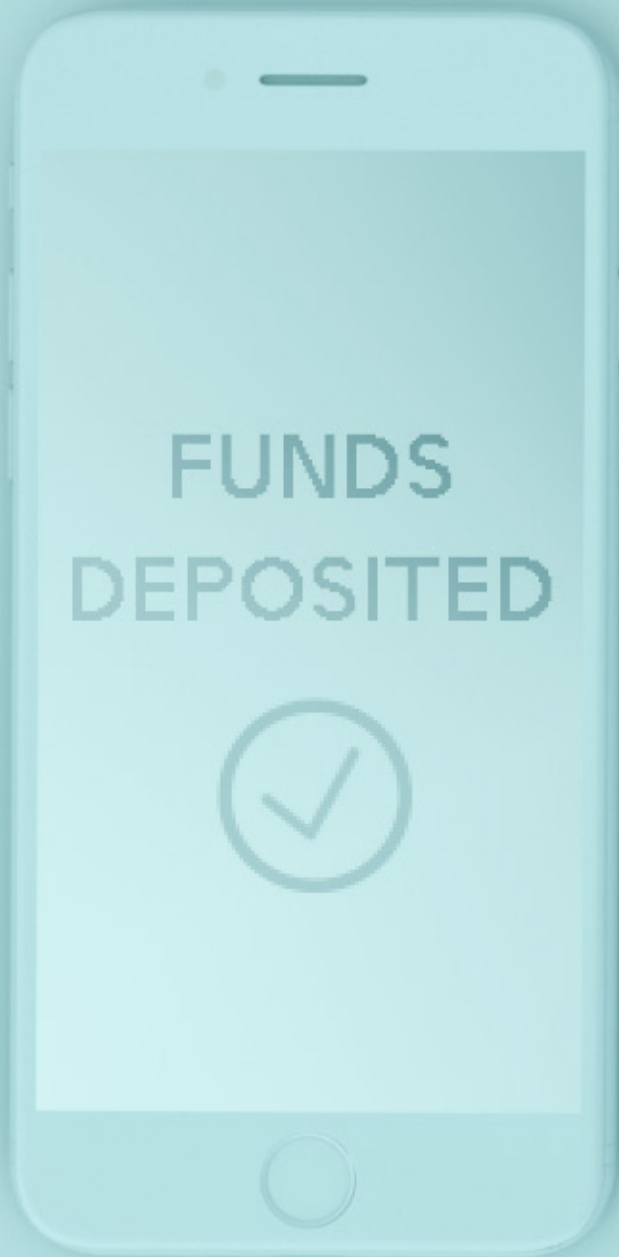
BATCH TOTAL **\$375**



The Settlement

Once a batch is closed, the *settlement* occurs when the processor receives the processed funds from each issuing bank whose credit cards were part of the batch. The total batch amount will then be transferred via bank-transfer to your bank account. How fast you receive a closed batch is up to your processor, as processors will sometimes place hold times on settlements to manage risk. Without holds, funds should appear in your bank account within 1-2 business days. Some processors have longer wait times and might make you wait 7-10 business days to receive your funds, while others may offer same-day deposits for a higher fee.

In the earlier days of credit card processing, each card-brand (Visa, Mastercard, etc.) would require a separate processor and financial arrangement. This required individual batches and settlements for each type of card, resulting in multiple bank deposits. Changes in laws allowed banks to issue and process multiple card types, letting processors offer merchant account arrangements that covered all major credit card types in one service. It is now very rare to see a processor that separates deposits by card type. The exception to this is for merchants who have accounts directly with Amex, in these cases their deposit will come directly from Amex.



Gross Settlements vs. Net Settlements

Some merchant accounts are configured for *gross settlements*, meaning that the total batch amount you processed will be deposited into your bank account for that day. The actual processing fees that applied to those transactions, and all other transactions that month, are then withdrawn from your bank account on the 1st day of the following month.

Other processors will choose to place merchants on a *net settlement* configuration. This means that instead of receiving their full batch amount, they will receive the full amount minus their processing fees.

An example of a Net Settlement:

Total Batch Amount	\$1,000.00
Processing Fee (2.9%)	-\$29.00

BANK DEPOSIT AMOUNT	\$971.00

RISK FRAUD & PCI

This portion of our guide is to help merchants understand the risks associated with credit card processing, identify fraud before it happens, deal with chargebacks when they occur, and protect your business with safeguards like PCI while still enjoying the benefits of accepting credit cards.



Understanding the Risks

Each entity in the credit card processing industry that is involved in a credit card transaction is exposed to unique risks. Understanding where the risks lies can help you reduce your exposure and better understand your role in protecting yourself and your business.

Risks for Issuing Banks

When banks issue credit cards to their customers, they are essentially extending credit. They cannot be sure that each cardholder will be able to repay their credit card balance. If a cardholder is unable to pay their credit card balance and defaults on their debt, the issuing bank will be taking a loss on that account and the balance owed. Issuing banks will mitigate their risk by doing personal credit checks on credit card applicants and setting appropriate card balance limits to define the amount of credit that a consumer is able to access based on their individual circumstances.

Risks for Acquiring Banks / Processors

Credit card processors bear the risks of merchants that are insolvent and are unable to repay chargebacks or penalties imposed by the card networks. To mitigate risks, processors use several techniques to reduce the likelihood that they have approved a merchant account for someone who will be unable to repay these penalties or who might be at risk of having high volumes of chargebacks or penalties. These techniques include credit checks on merchant applicants and monitoring transactions, throttling settlements speeds, and placing holds on funds. The nature of some businesses or industries is such that chargebacks may be more likely, and this is something that processors consider when approving a merchant account and determining processing rates.





Risks for Merchants

As a merchant, you are at risk for chargebacks and carry the financial responsibility of the potential reversals for transactions that you process. To mitigate this risk, you should monitor your transactions for suspicious activity and beware of fraudulent activity. We'll provide more details on how to avoid chargebacks later on in this section.

Cardholder Protections and Risk For Your Business

Cardholders are provided certain protections against the abusive or fraudulent use of their credit card. For example, if their credit card is stolen and used at merchant locations, they can call their issuing bank and have the charges reversed. They can also dispute charges for purchases that were never shipped, or where the goods or services received were not as described. The advantages of these cardholder protections are that they promote the use of credit cards and give customers the confidence to make purchases at locations they might otherwise not know or trust – essentially, promoting the easy flow of commerce.

However, as a merchant you need to understand that by accepting credit cards as a form of payment, you're putting yourself and your business on the other end of these cardholder protections. If a stolen credit card is used at your location, or a shipment fails to reach your customer, then you are liable for re-funding the original transaction. This is known as a chargeback, and it's where the financial risk of credit card processing comes from.

The single most important thing for you to remember is that you, as the merchant, are ultimately responsible for potential chargebacks.

If a merchant is careless or ignores warning signs, they may ultimately pay the price as transactions can be reversed, and the merchant stands to lose both the original transaction funds and the goods provided.

Balancing Fraud and the Flow of Commerce

If your business accepts credit cards, fighting fraud while also allowing legitimate transactions to flow seamlessly is an ongoing balancing act. Card networks want to encourage consumers to use their credit cards, but they don't want the cards to end up in the wrong hands or to be used by someone who is not the card's rightful owner.

Banks want to make it easy for people to access their money seamlessly whenever they need it and wherever they are, but they don't want to make it so easy that someone other than the account owner would be able to gain access to the funds.

As a business owner you will also want to make it easy for customers to make purchases using their preferred payment method, but because of the risks associated with fraudulent transactions and chargebacks that we mentioned in the previous section, you don't want to make it so easy that your transactions end up being disputed and you lose income to chargebacks.

Here is an example of this balancing act. An ecommerce store wants to require their customers to provide photo-ID before making an online purchase, as a way to reduce fraudulent orders, but this added friction would likely increase their shopping cart abandonment rates and result in less revenue. This highlights that balancing risk while encouraging business is an ongoing challenge in the world of commerce and it is ever evolving.

Merchant-Fraud

It is possible for merchants to commit fraud. Payment processors ask for business information and details when setting up merchant accounts for applicants to reduce their risk of being exposed to fraud. Processors are at risk for fraudsters who sign up for merchant accounts with no intention of operating legitimate businesses. In these cases, the accounts are sometimes used to process as many

fraudulent transactions as possible in a small period of time before the processor catches on and closes the account. To reduce the risks of these types of fraudulent accounts, processors may hold funds when a new merchant begins processing with them, or they may request additional details if there is a high-value transaction or processing activity that is outside the normal activities of a certain account or industry.

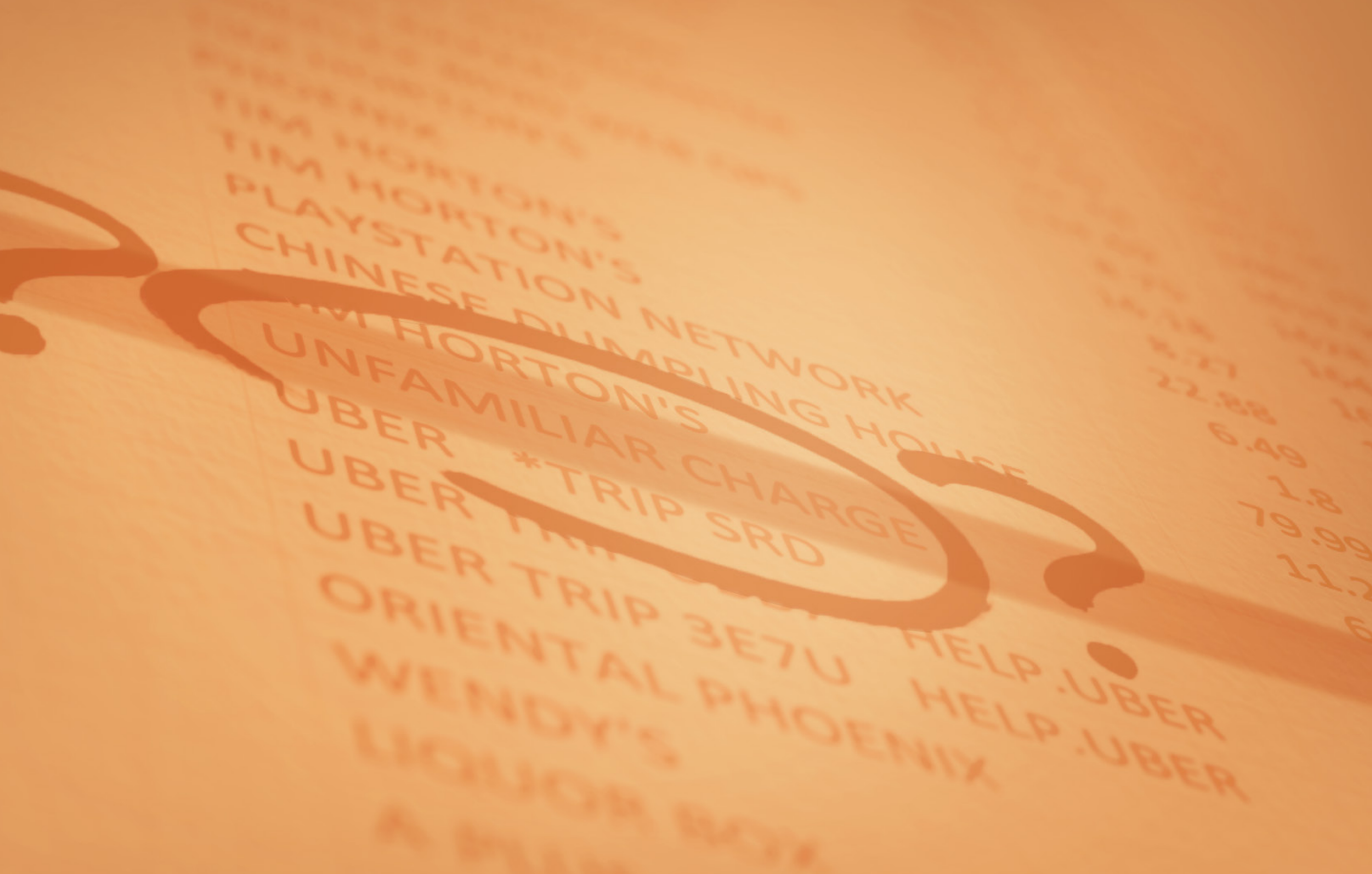
Some merchants also resort to identity theft to sign up for merchant accounts because they might not be able to qualify for one themselves. Or, if their business is considered high risk or illegitimate, in order to get their business approved, they might fabricate important details like what they are selling or what the core function of their business is.

Fraud and Other Risks Merchants Face

There are several different types of credit card fraud and risks that you should be aware of as a merchant. By making sure you understand the different types of risk that you might face, you'll be better equipped to know what to look for while processing transactions in order to protect your business.

Stolen Credit Cards

As a merchant accepting credit cards, you will want to minimize the likelihood that someone is able to use a stolen credit card to make a purchase from your business. If you process a transaction using a stolen credit card, then you're opening your business to the risk of a chargeback when the legitimate cardholder realizes that their card has been stolen and used for a purchase that they did not authorize. Using address verification (AVS), asking for the CVV for card-not-present transactions, requesting photo identification, or enforcing chip-card acceptance are all ways you can help minimize the risk that someone is using a stolen credit card.



Friendly Fraud

If a customer notices a charge on their credit card statement that they do not recognize, if they don't receive a product or service they order, or if the product or service they receive is defective or unsatisfactory, they can dispute the transaction and file a chargeback. In many cases, the customer may have unknowingly agreed to a recurring billing cycle, or they may have been genuinely confused about what they were purchasing. This would be considered *friendly fraud*, and even though it might not be intentional fraud, it can still harm your business as well as lead to other, more intentional forms of fraud down the line. Customers who commit friendly fraud do not usually have any malicious intent, they are often simply confused about the proper channels to use to request a refund or are forgetful about their purchasing habits. For these reasons, it is important for merchants to clearly identify their business name on credit card statements to avoid merchant confusion and have clearly posted communication channels for customers to ask questions and clarify purchases.

The resulting chargebacks from friendly fraud mean that the customer's financial institution cancels the transaction, the customer gets refunded in full, and the customer generally keeps the item or service they ordered. As the business owner, this means that you've now lost out on a sale, are out product or hours, and must incur the chargeback fee issued by the card brand.

▶ Chargeback Fraud

Chargeback fraud is often confused with friendly fraud, because the chargebacks filed are often for the very same reasons, but chargeback fraud is when a customer is *knowingly* exploiting consumer protections to their benefit. In these cases, a customer would initiate a chargeback after making a purchase using their own credit card even after receiving the item or service. Taking measures to protect your business from friendly fraud also protects you from chargeback fraud, so it's a good idea to take the necessary precautions.

Authorization Error

An *authorization error* may occur if you do not have approval from the issuing bank to process a transaction. You may also get this error if you process the same transaction multiple times in error, or if you process a transaction without approval, or with an approval code that is invalid.

Customer Dispute / Chargeback

A *dispute* occurs when a cardholder questions a payment made on their card with their card issuing bank and can sometimes lead to a *chargeback*. When a dispute occurs, you will be charged a chargeback fee, and the payment will be reversed. You will be able to respond to the dispute by submitting evidence to the card issuer to demonstrate that the transaction was legitimate and that the customer agreed to the purchase. If the card brand sides with your business then the transaction amount will be returned to your account (though the chargeback fee is usually not), but if the card brand sides with the cardholder then the payment will remain refunded to the cardholder.

Issuer Dispute

An *issuer dispute* can occur if the card brand is suspicious of a transaction, or if the transaction was not authorized because the cardholder account is in collections and the merchant did not obtain valid authorization to process the transaction.

Stolen Credit Card

If a transaction is processed with a credit card that has been stolen, then the original cardholder may file a dispute or a chargeback request after noticing that the unauthorized transaction was posted to their account. If the CVV, AVS, or customer details do not align with the details listed on the credit card, you can request additional details, ask for another payment method, or decline to process the transaction to help protect your business from the risk of processing a stolen credit card. If you are processing a large volume of online transactions, then you will likely want to confirm that the CVV and AVS details align with the customer shipping details.



▶ Understanding Chargebacks

There are two types of *chargebacks* that you might encounter, a *Retrieval Request* (also known as a Copy Request) or a *Chargeback Request*. A Retrieval Request is a non-financial request, it occurs when the credit card issuer contacts you to confirm information about a transaction. The reason for the request can be for a variety of reasons ranging from a customer question, incomplete transaction information, a processing error, or the suspicion of potential fraud. This type of request does not immediately result in a financial penalty and is just a request for information.

A Chargeback Request, on the other hand, is a financial request, meaning that your business will be debited because of the request. This occurs when the cardholder contacts their financial institution to dispute a specific transaction and requests a refund for a transaction. This could occur because the goods purchased never arrived, the goods arrived but varied from the customer's expectation, or the credit card was used without the cardholder's knowledge.



There are three reasons why a chargeback could be filed against your business:

1 CARDHOLDER DISPUTE

A cardholder might decide to dispute a transaction for a number of reasons including:

- Because it was fraudulent
- Because they want a refund and don't see another way to get it
- If they are dissatisfied with the product or service
- If they did not receive the merchandise
- If they don't recognize the transaction on their statement
- If they're trying to cancel a recurring transaction but aren't sure how to do it
- If they were unaware they were being billed for something

2 ISSUER DISPUTE

An *issuer dispute* will be initiated by the institution that issued the credit card, not by the cardholder. This will occur if the cardholder account is in collection status and you did not obtain valid authorization for the transaction.


3 TECHNICAL ISSUE

This occurs when there is something that is technically wrong with the transaction, this could be on either the issuer or the acquirer side, such as forcing a fake approval code.

| Chargeback Process

Here is an overview of how the chargeback process works from beginning to end if a chargeback is initiated by a customer of yours.

- 1 The chargeback process begins when your customer looks at their statement and notices a transaction that they do not remember, that they did not authorize, or that they believe has been processed in error. Once the cardholder notices the transaction of concern, if they do not contact your business first, they will contact their card issuer to dispute the transaction.
- 2 The card issuer reviews the dispute filed by the customer, determines if the claim is valid, and ultimately decides if the chargeback will be taken forward. If they determine the claim to be invalid, then the process would end here, and the cardholder would be notified. Keep in mind that the ability to file a chargeback is part of consumer protections that your customer benefits from by using their credit card, so the card issuer is likely to side with the consumer (who is also *their* customer).
- 3 If the chargeback was determined to be valid by the card issuer, they will then submit the chargeback to the card network involved for reimbursement. The card network will instruct your acquiring bank or processor to immediately withdraw the funds for the original purchase, along with a chargeback fee (usually around \$15 to \$25), from your account which will be used to refund the customer. This ultimately means that your business has reimbursed your customer the funds for the purchase and you will no longer have the proceeds from the transaction, along with the product sold or services rendered.

- 
- 4 When you receive notice of the chargeback, you'll also receive instructions on how to dispute the claim if you wish to do so. If you know that the chargeback has been filed in error and that the transaction is valid, you can provide supporting details and documentation to dispute the chargeback and make your case.
 - 5 After you have submitted your supporting documentation to prove the transaction was valid, the acquirer takes your documentation and submits it to the card network, who will then give it to the issuer to review.
 - 6 Once the card issuer reviews the documentation for the dispute, they will determine whether the documentation you provided was enough to disprove the cardholder's initial dispute, or if the customer was correct, and the chargeback will be upheld.
 - 7 If you lose the dispute, you can file for arbitration with the card network, but this will cost you upwards of \$500 or more. If you win the dispute, the refund is reversed, and you are reimbursed the funds for the initial transaction by the processor. Some processors will also refund the chargeback fee to you, but most will not, as it is usually a fee that they, themselves, need to pay to their backend acquirer. There is still a chance that the cardholder will dispute this outcome with a second chargeback and the process would begin again.

Dealing with a chargeback is likely the most unpleasant part of accepting credit cards for most business owners. Luckily the chances of receiving one are low, and understanding how chargebacks work and what your options are for disputing illegitimate claims will help you protect your business from additional costs.

Fighting a Chargeback

If a customer files a chargeback against your business that you do not believe is valid, you have 30 days to be able to submit a response to the chargeback. To be able to fight a chargeback you will need to compile relevant documentation that supports the validity of the transaction and write a response letter that speaks to the chargeback reason code. Be sure to look up the card brand's reason codes before writing the letter so that you can speak to the specific situation noted for the chargeback. Once all the information and the letter are compiled, you will submit them to your payment processor for review by the card network.

Each chargeback type and reason code will warrant different information to contest it. Some of the information and documentation that can assist in proving your case are listed below.

- ✓ *Date/time stamp for the transaction*
- ✓ *The device used*
- ✓ *Shipping verification*
- ✓ *CVV match for the transaction*
- ✓ *Device fingerprinting*
- ✓ *Geolocation*
- ✓ *Past transaction history*

Chargeback Arbitration

The chargeback case will go to *arbitration* when the issuer and cardholder are unable to come to an agreement with the acquirer and yourself about which party should be financially liable for the transaction during the pre-arbitration stage. At this point, if the chargeback claim is with Visa, then the issuer will file the arbitration case against the acquirer and yourself. If the chargeback claim is with Mastercard, then the acquirer will file the arbitration case against the issuer on behalf of your business.

Whether your chargeback claim is with Visa or Mastercard, they will be the ones who rule on the arbitration case filings and the losing member will be responsible for all associated fees, which could be quite costly to your business. Chargeback arbitration fees typically start around \$500 and can rise from there.

- ✓ *Subsequent transactions from the customer if applicable*
- ✓ *Any email communications or interactions with the customer*
- ✓ *Phone call transcripts*
- ✓ *Live chat transcripts*
- ✓ *Social media interactions and shares*

Protecting Your Business from a Chargeback

As payment processing technology advances, new card security features, online security options, and secure software all help protect your business while still allowing you to freely accept credit cards. As a merchant, there are steps you can also take to protect your business from the risk associated with chargebacks.


Listed below are some responsible measures you should be taking for your business.

- ✓ *Have a comprehensive and clearly stated return policy.*
- ✓ *Ensure all product descriptions are accurate and clear to set appropriate customer expectations.*
- ✓ *Make it clear to customers how they can contact customer service if there ever is an issue. Be sure to respond quickly and professionally to any issues that may arise.*
- ✓ *Ensure any and all records of all transactions and communications with customers are stored. The more relevant information you gather, the easier it will be to defend yourself against false claims.*
- ✓ *Provide tracking numbers and require customers to sign for the delivery of ordered goods.*
- ✓ *Have a clear description of your company show up on customer bills and statements so customers can easily and clearly reconcile their purchases with your business.*

How to Evaluate the Legitimacy of a Transaction

There are steps that you can take to mitigate the risk of fraudulent transactions and processing stolen credit card numbers. We've provided a comprehensive list of ways you can fight fraud, but keep in mind that these steps do not need to be completed in any specific order, and not all steps will apply to every transaction.

What's important to remember is that by keeping an eye out for common red flags and suspicious patterns, you are better equipped to be vigilant and protect your business. If there is a transaction that you are not comfortable processing, then you can always void or refund the credit card and notify the customer.



When evaluating a transaction for its legitimacy ask yourself these questions:

1 HAS THERE BEEN A SERIES OF DECLINED ORDERS WITH THE SAME SHIPPING ADDRESS?

Fraudsters often have a list of stolen credit cards and will try each one until they get an approved transaction. Be vigilant for series of "DECLINED" and "PICK UP CARD" notices.

2 HAVE THERE BEEN PRIOR CHARGEBACKS FROM A SIMILAR ADDRESS OR LOCATION?

Certain countries and regions have large fraud problems and many online retailers refuse to ship orders to those regions. Look for patterns based on your previous chargebacks and make decisions on what you will allow. If fraudulent orders to a specific country go over a certain %, strongly consider banning that country from purchasing from your online store.

3 ARE THERE MULTIPLE ORDERS FOR THE SAME CUSTOMER USING DIFFERENT CREDIT CARDS?

Be on the lookout for multiple orders with the same shipping address but different credit card numbers.

4 DID I REQUIRE THE CVV DURING THE PAYMENT/CHECKOUT PROCESS?

There are no longer any major card brand credit cards without a security code on the back. If you are manually entering your customer's card information, you should always ask for and enter the CVV code. If your customers are entering their own information during the checkout process, you should require the CVV code and not allow the security check to be bypassed. Just remember to never record or make note of the CVV, as it is a violation of the PCI requirements.

5

IS THE TRANSACTION SIZE OR THE ITEMS PURCHASED OUT OF THE ORDINARY?

Often fraudsters will purchase items that they can resell, like a specific shirt of every size or color, or a larger number of the same item. Compare every new order with previous ones and be wary of orders that don't fit with the rest. Very large transactions that seem too good to be true often are.

6

DOES THE SHIPPING ADDRESS MATCH THE BILLING ADDRESS?

Although it can have somewhat of an impact on legitimate sales, by only allowing the shipping destination to be the same as the billing address, you can greatly reduce your exposure to fraud. Fraudsters will often use the billing address of the stolen cardholder but will put their own address as the shipping destination. If you do not wish to enforce this limitation, make sure that the shipping address is at least within the same city, state/province, or country depending on your risk threshold.

7

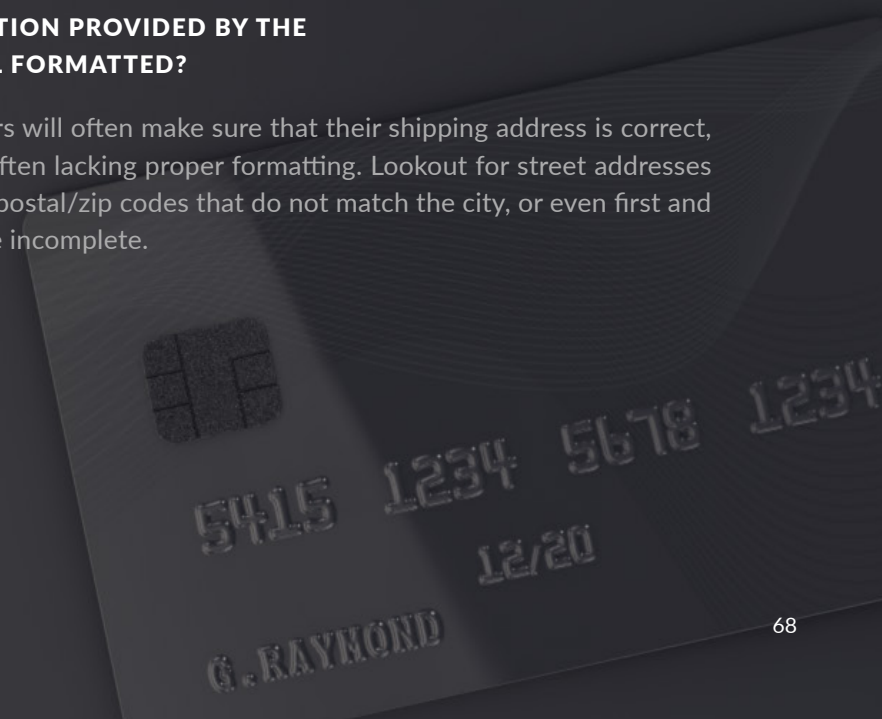
ADDRESS VERIFICATION SERVICE (AVS)

The address verification service (AVS) takes the street address (one line) and the postal/zip code and compares it with what the cardholder's bank has on file. Chargebacks with an AVS response of X, Y or Z are most often ruled in favor of the merchant if you have a proof of shipping delivery to that specific address. However, this does not apply if the chargeback was because of a dissatisfied customer (as opposed to a stolen credit card).

8

IS THE INFORMATION PROVIDED BY THE CUSTOMER WELL FORMATTED?

Although fraudsters will often make sure that their shipping address is correct, the billing info is often lacking proper formatting. Lookout for street addresses without numbers, postal/zip codes that do not match the city, or even first and last names that are incomplete.



9

DID YOU CALL THE CUSTOMER? DOES THE TELEPHONE AREA CODE MATCH THE ADDRESS?

A simple courtesy call to the customer to confirm their order and address will often give you a better sense of the legitimacy of an order. Are they nervous or dismissive? Do they challenge you when asked to confirm their information? The area code of the telephone number can also help in making sure that the customers are within the same region as their billing and shipping address.

10

AVOID SHIPPING ORDERS TO PO BOXES.

Keep in mind that postal offices in some rural areas do require a box number. However, PO Boxes for major cities should generally be avoided.

11

DOES YOUR SHIPPING COMPANY REQUIRE ID OR SIGNATURE UPON DELIVERY?

For international orders and transactions without proper AVS results, consider asking your shipping provider to require an ID or customer signature before delivering the package. Some shipping companies will also provide you with a copy of the signed delivery receipt.

12

DOES THE SHIPPING/BILLING ADDRESS MATCH THE COUNTRY OF THE ISSUING BANK?

The credit card BIN (the first 6 digits of the full credit card number) will provide you with the specific bank that issued the credit card. Perform a BIN lookup to receive the contact information for that specific bank. Is the customer in the same country as the bank that provided them with the credit card? If you aren't sure about a transaction, try contacting the bank's risk department and let them know that you have doubts about the transaction. They might be willing to perform a courtesy call to the customer to confirm the purchase.

PCI Compliance

PCI DSS (Payment Card Industry Data Security Standard) is a set of standards designed to ensure that credit card information remains safe and is captured, transmitted, and stored in a safe and secure way. In other words, it is a set of rules to reduce the risk of fraudsters, hackers, and thieves from stealing sensitive credit card information.

Who does it apply to?

PCI compliance applies to *all businesses* accepting credit and debit card payments, regardless of their size or their nature. Even small merchants using a mobile app on the weekend are required to meet PCI standards. PCI is the world's largest security standard, as it applies to millions of merchants, processors, ATM companies, and other service providers world-wide.

Who sets the standard and who enforces it?

The Payment Card Industry Security Standards Council (PCI SSC) is the governing body that sets and updates the standard. It was created in 2006 by the major card brands, including Visa, Mastercard, Discover, and American Express in order to have a universal set of rules. The card brands are the ones that enforce the standard, requiring processors to be compliant, validate their merchants, and impose fines if a breach occurs because of non-compliance.

Why do I have to be compliant?

To avoid getting breached and losing credit card numbers. Fines imposed by the card brands in the event of a breach can be extremely costly to your business. In this digital age, all businesses should want to protect themselves. By being compliant you also gain access to extended breach coverage. Prepare your business for compliance by visiting the PCI Security Standards Council or speaking to your payment processor.



My provider is compliant, does that mean I'm compliant?

The short answer is no. It is required for all payment service providers to be PCI-DSS Level 1 compliant, but merchants are still responsible for the security scope of their own business environment. A virus-infected computer or a dishonest staff member is all it could take to have someone steal credit card numbers from your business. We recommend that merchants use as many compliant services as possible that help shift that scope of responsibility. These include using your provider's credit card vault, using card readers and terminals that offer end-to-end encryption (E2EE), using hosted payment pages and .js payment plugins, and whatever other tools are available to shift your PCI liability over to your service provider. But even with a reduced security scope, merchants must still complete a basic self-assessment questionnaire (SAQ) once per year, attesting their compliance on this final scope.

Becoming PCI Compliant

Most payment processors provide a pathway for their merchants to become *PCI compliant*. Often, this involves giving their merchants login access to a third-party PCI manager portal, allowing them to complete a once-per-year self-assessment questionnaire (SAQ) and receive their PCI certificate.

However, some payment processors have chosen to turn a blind eye to the compliance of their merchants. This is especially common with some of the payment facilitators who deal with smaller merchants. The down-side of this approach can be severe to the merchants. In the event of a breach – such as the merchant’s computer being stolen and credit card numbers are lost, or a dishonest staff member of the merchant’s steals credit card number - no protection is offered to the merchant.

Helping small businesses become PCI compliant can be somewhat cumbersome and expensive, which is likely why some processors prefer to ignore it. But the consequences of not being compliant ultimately fall on the merchant. Choosing a processor that is willing to help you become PCI compliant will ultimately put your business in a safer place.





PCI Compliance and Non-Compliance Fees

Fees related to PCI compliance are entirely determined by the payment provider that you choose. The card brands (Visa, Mastercard, etc.) do not impose any monthly or annual PCI-related fees (outside of the actual final penalties in the event of a breach).

PCI Compliance Fee (with a PCI Program)

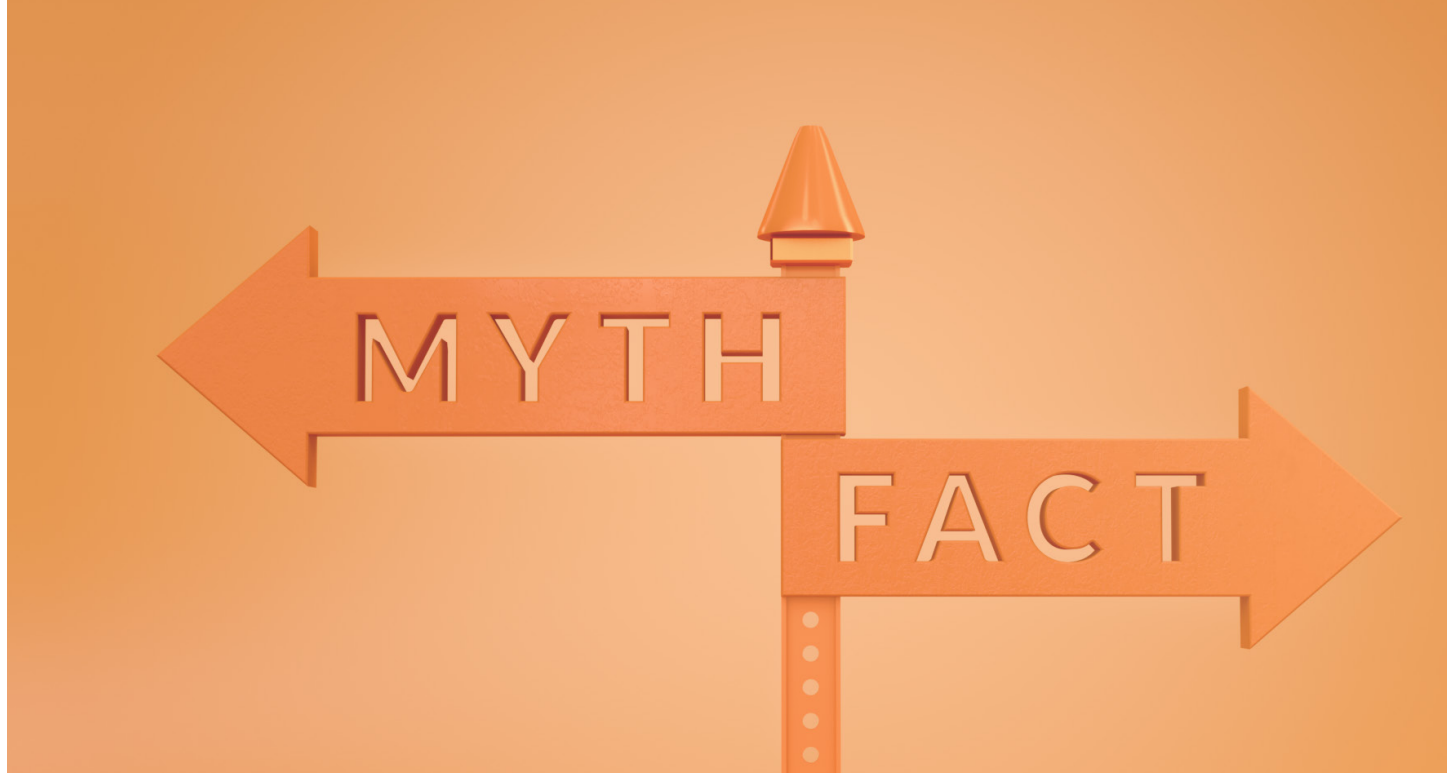
Some processors choose to charge merchants for access to their PCI compliance program. This is usually in the form of a monthly, quarterly, or annual *PCI compliance fee*. Other processors may provide this service without charging additional fees to the merchant.

PCI Compliance Fee (without a PCI Program)

Some processors charge a PCI compliance fee, but without access any kind of PCI compliance program or portal. This is unfortunately quite common and creates a false sense of security with merchants thinking that paying the fee has made them compliant. Any processors charging for a fee for a service without actually delivering that service should be viewed as highly suspect in their billing practices.

PCI Non-Compliance Fee

To encourage merchants to complete their annual PCI compliance requirements, some processors charge a non-compliance fee or penalty, usually after 90 days of non-compliance. Merchants need to complete their self-assessment questionnaire to avoid this fee. While unpleasant, this fee is often used as a motivator to increase PCI compliance and the overall security of merchants.



Myths About PCI Compliance

PCI Compliance is an often-misunderstood aspect of payment processing, especially for business owners who are new to accepting credit cards. Many payment processors don't want to talk about PCI because while it is not *law* as such, the consequences of being non-compliant can be serious and potentially very damaging to your business. Understanding how PCI Compliance works and recognizing if someone is sharing false information with you can help you protect your business from costly data breaches and fines. Here are some of the common myths surrounding PCI compliance that you should be aware of.

MYTH: My business is still quite small, so I don't need PCI.

FACT: If you accept credit cards then you need to be PCI compliant.

MYTH: I don't have an online store, so PCI doesn't apply to me.

FACT: If you are accepting credit cards in any manner or storing or transmitting cardholder information, then you need to be PCI compliant.

MYTH: I'm mostly compliant, so that's good enough.

FACT: PCI compliance is all or nothing. If you do not meet the criteria 100% then you are not PCI compliant and would not be considered so.

MYTH: I can just answer "Yes" on the questionnaire, so I pass.

FACT: Answering "Yes" to a question when you should have said "No" exposes your business to even greater risk if a breach were to occur because you have misrepresented your business's security.

MYTH: PCI is too hard.

FACT: PCI can seem daunting at first, especially as a new business owner. However, because PCI is based on the best practices for security, these are steps that you should be taking anyways to protect sensitive data and your business.

MYTH: I outsource my credit card processing, so I don't have to worry about PCI.

FACT: Even if you're using a third-party for your credit card processing, you still need to be PCI compliant to protect your business. Credit card processors need to adhere to a multitude of PCI compliance measures as well.

MYTH: PCI doesn't stand for anything specific.

FACT: PCI stands for payment card industry. PCI-DSS stands for Payment Card Industry Data Security Standard.

MYTH: PCI is just a cash grab.

FACT: The purpose of PCI is to reduce a merchant's exposure to potentially fraudulent activity and to protect them in the event of a data breach. A [2017 Verizon Data Breach Incident Report](#) found that there were nearly 42,068 data breaches in 2017. Breaches are not often publicized but they can have devastating financial consequences for your business, especially small businesses. Most businesses aren't aware of these consequences, so PCI was implemented to protect all businesses who accept credit cards.

MYTH: I did my PCI compliance when I first started my business, so I'm good.

FACT: A PCI certificate expires every 12 months and needs to be renewed each year.

MYTH: If I'm not compliant then my transaction fees are going to increase.

FACT: While you may be subject to a PCI Non-Compliance Fee from some processors, your transaction fees should not change if you are non-compliant unless your processor chooses to bury their PCI fees in your rates without informing you. Unfortunately, some processors employ this method instead of simply educating their merchants on PCI.

MYTH: PCI Non-Compliance Fees are just a small flat rate.

FACT: PCI Non-Compliance Fees may vary depending on who your payment processor is, and they may issue the fee as a flat rate fee or as a percent of your processing volume. How a processor applies the fee can result in a large variance in what they are charging, and if your processor isn't transparent about how and what they're charging you, it may be difficult to recognize.

While understanding PCI won't make it any more enjoyable to adhere to, it can help you protect your business from expensive data breaches and related fines by ensuring you're meeting the required security standards and helping you avoid unnecessary monthly fees for PCI Non-Compliance.

Thank you

Congratulations! You've completed our *Merchants Guide to Credit Card Processing*. Be proud! That was a lot to get through!

You now have a stronger understanding of how credit card processing works, how to choose a payment processor, what equipment might be best for your business, and how to accept credit cards while protecting your business from fraud and other risks.

Armed with this knowledge, you're ready to take on the world of payments. You're more informed on how to do what's best for you and your customers. You also have the knowledge needed to protect your business from some of the potential risks associated with using credit cards by preventing and identifying fraud before it happens.

If you'd like to learn more about credit card processing, we post regularly on the Helcim Blog on a variety of topics to help your business grow. Check out our blog [here](#).

Looking for A Processor?

If you are looking for a new payment processor, Helcim is committed to providing a better payment experience. With Helcim, merchants benefit from low processing fees, instant sign-up, friendly in-house customer service, and all-in-one software offering. Our merchant services and business software are designed to put merchants first by simplifying your business operations and keeping your credit card processing easy, efficient, and affordable.

If you are new to credit card processing, let us help you get started on your journey the *right way*. The world of payments can be a doozy if you partner with a processor who isn't looking out for your best interests. We unfortunately deal with merchants every day who reach out to us wanting to switch because they've had negative experiences with their current or past processor. At Helcim, our commitment is to provide the best and most affordable payment experience possible in a fair and honest way.

If you'd like to learn more about Helcim or get started with payment processing contact the Helcim Gurus who are always happy to help in any way they can. We provide complimentary rate comparisons and honest advice about what processor will be best for you and your business. Happy Processing!

-The Helcim Team

www.helcim.com

GETTING TO KNOW THE TERMS

The credit card industry is full of acronyms and terms. Here are some important ones:

▶ ACQUIRING BANK

The merchant's acquiring bank. Sometimes the same as the processor, this is the bank in the background that approves and underwrites the risk of the merchant account and provides funding.

BATCH

A group of credit card transactions processed for the day or a period of time.

CARDHOLDER

The customer that possesses the credit card.

CARD BRANDS/CARD NETWORK

The credit card brands that operate the network. These include Visa, Mastercard, American Express and Discover Card.

CARD-NOT-PRESENT

When the customer and their card is not physically in the merchant's presence when a transaction is processed, such as an ecommerce transaction.

CARD-PRESENT

When the customer and their card are physically present for a transaction.

▶ CHARGEBACK

An event where a customer files a complaint with their bank to be refunded a credit card transaction. This could be because their credit card was stolen, or they did not receive the purchased goods.

CREDIT CARD NUMBER

The 15 or 16-digit credit card number, shown on the front of the card.

▶ CVV/CVC/CVD

The 3 or 4 digit security code, usually found on the back of the credit card.

DISCOUNT RATE

The percentage (%) charged on each transaction as part of the processor's payment fees. A confusing name, it comes from the fee-amount "discounted" from the transaction's original total.

▶ EMV / CHIP & PIN

EMV refers to the new credit card Chip standard. It standard for "Europay Mastercard Visa" who were the three cards that originally developed the technology.

EXPIRY DATE

The expiry date (formatted MMY) of the credit card.

▶ ISSUING BANK

The customer's credit card bank. This is the bank that issued them the credit card.

MAGNETIC / SWIPE DATA

The credit card information that is stored on the magnetic stripe (or magstripe) on the back of the credit card.

MERCHANT

The business accepting the credit cards.

▶ MERCHANT ACCOUNT

The account provided to a merchant that allows them to accept credit card payments.

MOBILE READER/CARD READER

A device that allows credit and debit cards to be accepted when paired with another device, such as a phone, tablet or computer.

▶ NFC

In a payments context, NFC (Near Field Communication) refers to the technology that has recently been integrated into payment processing infrastructure (credit and debit cards, phones, wearable devices, as well as card readers and terminals) that allows for and facilitates contactless payments. These payments are sometimes referred to as *Tap & Pay* or, simply, *tap*.

▶ PCI

PCI-DSS stands for Payment Card Industry Data Security Standard. It is a set of rules enforced by the card brands for the safe-keeping and safe-transfer of sensitive credit card information.

PROCESSOR

The credit card processor, providing the merchant account and the credit card processing service to the merchant.

SETTLEMENT

When processed funds from credit card transactions are sent to the merchant's bank account.

TERMINAL

A credit and debit card machine, usually capable of processing Swipe and Chip & Pin transactions and printing receipts.

▶ TOKENIZATION

A processor will store and encrypt a credit card and provide a token back to the merchant so that the card can be used at a later time without the merchant having to store sensitive credit card data.

▶ VIRTUAL TERMINAL

A web-based software used to process keyed-in credit cards using a web-browser, mobile phone and/or computer.



Find out more about how Helcim can help your business do more.

1-877-643-5246 | help@helcim.com