Century BUSINESS SOLUTIONS™

THE ULTIMATE GUIDE TO Payment Security

How to Minimize Payment Risk, 3 Simple Ways to Protect Your Payments, & More

✷ Security checklist included!

Table of Contents

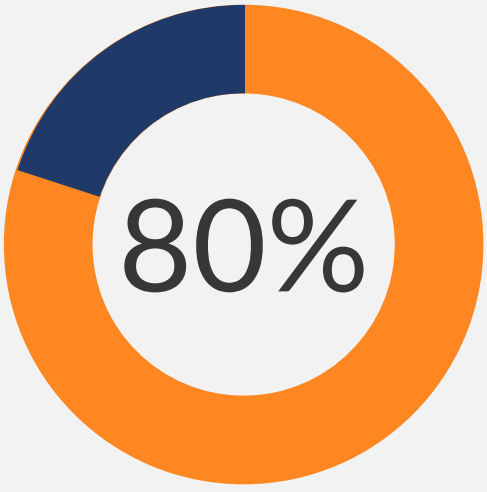
Introduction

Payment security is absolutely essential for any business that accepts credit cards.

Whether a customer gives their information over the phone, types their information into an online form, or swipes their card through a terminal, they're acting by faith. They expect their data to be safe, and they expect you—the merchant—to protect that data.

But merchants don't always take payment security seriously. According to the Verizon 2015 PCI Compliance Report, 80% of organizations are not PCI compliant. That number is frightening—especially since data breaches are on the rise and appearing in news headlines more and more often. According to the Identity Theft Resource Center Data Breach Report 2016, there's been a 40% increase in data breaches since 2015.

So what can you do as a merchant to keep your customers' data safe? You can start by learning about payment security and the steps you need to take to prevent fraud. That's why we created *The Ultimate Guide to Payment Security*—this guide will give you an overview of how you can be proactive in the fight against fraud, protect customer data, and take charge of your company's payment security.



of organizations are not PCI compliant

Verizon 2015 PCI Compliance Report

How to Minimize Payment Risk

Payment risk refers to the risk of loss in relation to payments, which can include a variety of different factors. Many companies that process online payments attempt to manage their own payment risk. However, getting outside help from a fraud prevention expert is often the best line of defense against fraud.

In order to fully minimize payment risk, it's best to use a payment gateway that provides fraud prevention tools. This way, instead of managing the risk yourself, you'll pass it on to a company that specializes in risk management. Your payments will be better protected and you won't have to worry about financial risk.

With the help of a risk management specialist, your business will be better protected from fraud. However, it's still important to have a general knowledge of payment risk to help prevent it before it occurs. This security guide will give you the crucial tools you need to help minimize payment risk for your business.

You could pay up to

$100,000

per month in fines if your business is not PCI compliant

PCIComplianceGuide.org

3 Simple Ways to Protect Your Payments

Without proper data security, your business could be extremely vulnerable to hackers and thieves.

As data breaches become more common, consumers are becoming more cautious with their shopping habits. They're unlikely to purchase from stores that look small or unprofessional, and even when they purchase from big-name stores like Amazon or Walmart, they're always thinking about data security.

If your store doesn't have the security necessary to protect customer data, then consumers won't buy. They'll avoid your store in favor of more established brands with better security.

There are three main reasons why merchants should worry about data security:

- To give your customers peace of mind
- To protect yourself from liability and damages
- To improve your trustworthiness and therefore your sales

With that in mind, here are 3 simple ways to protect your payments:

1 PCI compliance

The PCI DSS, or Data Security Standard, is a set of rules and standards for businesses to follow to make sure they're safely storing customer credit card information. The PCI DSS applies to any business that accepts or stores cardholder data, regardless of size or transaction volume.

The PCI DSS was developed by the PCI Security Standards Council, a group formed by the five major payment card brands (American Express, Discover, MasterCard, Visa, and JCB). The council was created to improve data security standards for credit card payments, educate businesses, and hold companies accountable to the DSS to help keep customer credit card data safe.

If a data breach occurs, PCI compliance lessens your business's liability. However, according to the Verizon 2015 PCI Compliance Report, 80% of organizations are still not PCI compliant.

In the event of a data breach, noncompliance could result in steep fines from the PCI Security Standards Council. If you're not PCI compliant, your business could pay up to $100,000 per month in fees, and your bank may end your relationship or raise the cost of transaction fees.

In addition, non-compliance can make your business more vulnerable to financial attacks and data breaches.

Cost of average data breach:

$3.62 million

Per lost or stolen record:

$141

2017 Cost of Data Breach Study, IBM and Ponemon

According to the 2017 Cost of Data Breach Study from IBM and Ponemon, the average cost of a data breach is $3.62 million. That's approximately $141 per lost or stolen record.

In fact, in over 10 years of research, none of the companies breached during Verizon's investigations were fully PCI compliant.

To make sure your business adheres to all PCI compliance guidelines, find a payment processor that uses encryption and tokenization technology to secure card transactions at every stage of the payment process. These extra layers of security prevent card information from being stored in its original format, drastically reducing legal and financial responsibilities for your business, and ensure that you remain PCI compliant.

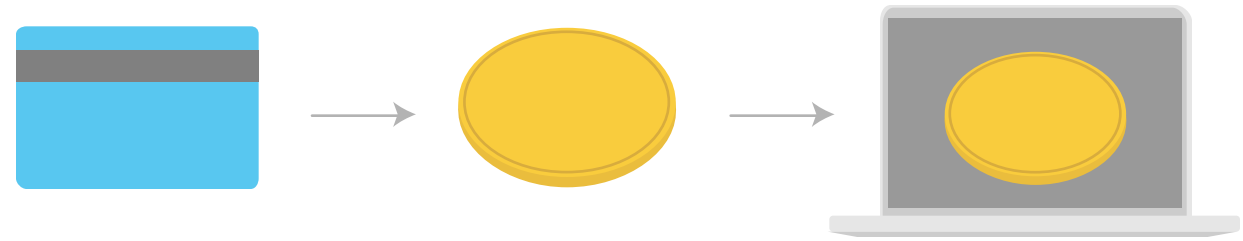
2 Tokenization

Tokenization protects credit card data when it's in use or in storage. How does it work?

The customer's credit card data is replaced with a token (an arbitrary string of numbers and letters) that stands in for the original information.

The merchant stores this token on their system, and the original credit card data is

no longer used for future transactions. That way, if the merchant's data is hacked, the thieves will only find valueless tokens that they can't use. Tokenization makes it impossible to hack or decipher your customers' credit card data and securely protects your customers' sensitive credit card data at all times.



While the possibility of fraud exists, tokenization keeps sensitive credit card data as safe as possible. Businesses can safeguard data against fraudulent activity by choosing payment gateways that use tokenization.

Tokenization is a growing technology that can save businesses millions of dollars in fraud liability while shielding consumers from data theft. Tokenization will be an essential player in the world of data security as credit card terminal technology has reached its threshold.

To make sure your customers' information is tokenized when they buy from your business, look for a payment processor that uses tokenization.

3 Cloud-based payment gateway

It's also important to find a payment processor that uses a cloud-based payment gateway. Cloud-based gateways store sensitive credit card data offsite on PCI compliant servers for maximum transaction security.

Because cloud-based gateways keep sensitive data off of your own server, you don't have to manage data security yourself, and you won't be held liable for data breaches.

The cloud also saves backups of all your data in case of disaster. If a catastrophic event occurred—for example, if a fire broke out in your office and everything was lost—your data would still be safe, kept on the offsite cloud server.

Another advantage of the cloud? Cloud-based accounting, which provides a secure method of finance management.

Cloud-based accounting software solutions allow businesses to access data from anywhere via the Internet, while offsite servers protect businesses from system administration costs and server failures. Most cloud-based accounting software solutions are also PCI compliant, which helps protect credit card information in the event of a data breach.

According to Firm of the Future, most cloud-based accounting software solutions are run from data centers, which offer multiple levels of security to protect both the software and your data. The typical data center has significantly better security than most small and medium businesses.

Conclusion

These three simple steps—PCI compliance, tokenization, and a cloud-based payment gateway—will give you the solid foundation you need to prevent fraud. With these measures in place, you're well on your way to building a comprehensive strategy to protect customer data.

40%

increase in data breaches since 2015

Identity Theft Resource Center Data Breach Report 2016

How to Prevent Fraud

When it comes to fraudulent activity, merchants should be aware of the vulnerabilities they face and how to combat payment fraud.

One of the best steps to take as a merchant is to start using a cloud-based payment gateway and integrated accounting software. Here are 5 simple steps to help protect your business from payment fraud:

1 Eliminate paper checks and invoices

Paper checks and invoices contain valuable information about your company and your customers. In the wrong hands, they can easily be used to commit fraud. It's best to eliminate them completely.

Instead, begin using a cloud-based payment gateway to keep your sensitive data secure. Cloud-based payment gateways allow you to securely access your information from anywhere. You can also send online invoices to your customers and manage payments from your laptop or smartphone.

2 Automate your payment process

A cloud-based payment gateway can automate your payment process and eliminate the need to input data manually. Your information is securely stored for future use, saving time and eliminating double data entry. Ultimately, you'll streamline workflow while protecting your payments.

3 Integrate your payment software

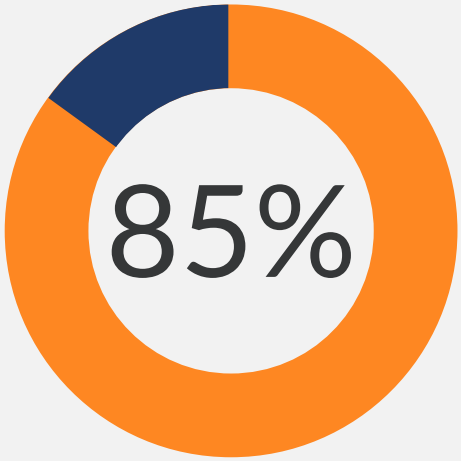
Integrated solutions allow businesses to process payments directly in their accounting software, providing a more secure method for managing finances. Integrated solutions can also improve your workflow, reduce overall expenses, and lower the risk of human error. Everything is done within a cloud-based payment gateway, which means your business will function as securely and efficiently as possible.

4 Be proactive

At the end of the day, you know your business best. Make a list of where you believe fraud is most likely to occur. Make sure to include clear standards of behavior in your employee manual, and train your entire team on how to protect customer data from fraud.

5 Take inventory

Keep tabs on your business and do internal audits on a regular basis. Consider hiring an outside accountant to do an independent review of your system.



of worldwide data breaches occur in the U.S. each year

Breach Level Index

Chargeback Management

What is a chargeback?

Essentially, a chargeback is protection for the cardholder. A successful chargeback is a reversal of a charge on a customer's credit card—that is, the money leaves the merchant's bank account and is credited back to the customer's card.

The reversal process begins when a cardholder files a complaint about a strange transaction on his or her billing statement. Upon receiving the complaint, the card issuer (a bank, for example), investigates the transaction in question.

If the card issuer concludes its investigation and finds the transaction to be fraudulent, the charge under review is reversed and the merchant incurs an additional chargeback fee (up to $100) in addition to losing the money from the sale and the value of the goods or services they rendered.

over

5.8 billion

breached records every year

Breach Level Index

Preventing chargebacks

As a merchant, you *can* control some of the factors that may cause a chargeback: your speed in delivering a product, your effectiveness in communication, your return policy, etc.

Therefore, the best way to prevent chargebacks is to be very communicative, attentive, and transparent about your products and policies. Eliminating inefficiencies in communication, unclear advertisements, and the like will reduce the number of customers who complain to their card issuers and initiate chargebacks.

Surveilling for fraud

Of course, some circumstances that lead to chargebacks—like credit card fraud—are out of your control. Fraud isn't completely preventable, but you can

certainly keep an eye open for anything that looks suspicious.

Here's a short list of suspicious activity to be on the lookout for:

- Large orders, beyond the scope of what's considered normal for your company
- New customers ordering very expensive items, especially if rush-requested or overnighted
- Multiple orders in a short period of time
- Billing and shipping addresses that don't match
- Order attempts with multiple (different) card expiration dates
- Multiple orders made with several credit cards but shipped to a single address

Seeing activity like this isn't always a clear indication of fraud, but it's better to be safe than sorry.

Investigate anything that looks out of the ordinary. If something feels suspicious, approach the customer who placed the order. Be friendly and transparent.

If you stop fraud at its source, you'll avoid the chargebacks that will inevitably come from those bad transactions.

1,091

data breaches were reported in the U.S. in 2016

Identity Theft Resource Center Data Breach Report 2016

Payment Security Checklist

In order to keep customer payment information safe, it's important to make sure that your business is up to date on the latest security measures. Here's a checklist of essential security measures that every business should use:

☐ Encryption

Encryption is the strongest protection for credit card data when it's in transit.

From the moment a card is swiped or inserted at a terminal featuring a hardware-based, tamper-resistant security module, encryption protects the card data from fraudsters as it travels across various systems and networks.

Encryption is ideally suited for any business that processes card transactions in a face-to-face or card-present environment.

☐ Tokenization

Tokenization protects sensitive credit card data at every stage of the transaction process. Card data is replaced with a unique token that's stored on the merchant's system. If a hacker accessed this system, the tokens would be valueless.

☐ PCI compliance

PCI compliance is at the forefront of payment security and secures the sensitive digital elements that fuel payment acceptance.

PCI compliance combines multi-layered security screening and proactive account monitoring with advanced tokenization and encryption technology to prevent cyber fraud.

☐ Off-site data storage

Make sure to use a cloud-based payment gateway that stores sensitive credit card

data offsite on PCI compliant servers. A cloud-based payment gateway keeps credit card data off of your own server so you don't have to manage data security

Integrated payments

Integrated credit card processing allows your business to link your accounting solution to a payment provider so you can process payments directly in your accounting solution. It also gives you access to cloud-based accounting, which provides a more secure method of managing your finances.

Cloud-based accounting software solutions allow businesses to access data from anywhere via the Internet, while offsite servers protect businesses from system administration costs and server failures. Most cloud-based accounting software solutions are also PCI compliant, which helps protect credit card information in the event of a data breach.

Fraud prevention features

Use a payment gateway that employs fraud prevention features built on a module stack design.

In module stack design, each module controls a different aspect of security so you can choose which modules to include in your stack.

Some examples of modules include: duplicate transaction control, block by country, block by IP address, and many more. The module stack design lets you add or change your fraud modules depending on your unique security needs.

Transport layer security (TLS)

All communication and processing in your payment gateway should occur through Transport Layer Security (TLS). TLS enables privacy between communicating applications and their users on the Internet.

To ensure the highest level of security, make sure to find a payment gateway that uses a 2048-bit RSA key and does not support ciphers known to be vulnerable.

Store credit cards individually

Use a payment gateway that stores each credit card number individually, making it impossible to steal an entire list or database full of sensitive data.

In this type of system, credit card numbers can only be viewed on an individual basis by unlocking or decrypting each one. If a card number is needed, the requested number is decrypted and unparsed from the system, a process that takes only a few seconds.

Third-party security scanners/assessors

Use a payment gateway that works with multiple third-party security companies to uphold the strictest security standards.

Every security assessor that works with your payment gateway should provide a certification that confirms your payment gateway meets all necessary security standards.

Identification through secure source keys

Use a payment gateway that offers a merchant toolkit with secure source keys.

Each merchant toolkit should communicate with the gateway using a unique high-bit encrypted string called a key. When information is sent to the gateway, the key identifies not only the merchant, but also the specific toolkit from which the information originated. You can use a separate key for each individual toolkit for enhanced security and revoke keys if you notice they're being misused.

Payment Security Checklist

- [ ] Encryption
- [ ] Tokenization
- [ ] PCI compliance
- [ ] Off-site data storage
- [ ] Integrated payments
- [ ] Fraud prevention features
- [ ] Transport Layer Security (TLS)
- [ ] Store credit cards individually
- [ ] Third-party security scanners/assessors
- [ ] Identification through secure source keys

Sources

Identity Theft Resource Center
Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout
http://www.idtheftcenter.org/2016databreaches.html

IBM Security
Cost of Data Breach Study
https://www.ibm.com/security/data-breach/index.html

PCI Compliance Guide
https://www.pcicomplianceguide.org/faq/

Verizon PCI DSS Compliance Report
http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf

Breach Level Index
http://breachlevelindex.com/

Firm of the Future
Are Cloud Accounting Applications Right for You and Your Clients?
https://www.firmofthefuture.com/content/cloud-computing-benefits-and-risks-of-cloud-accounting/

Century Business Solutions
Credit Card Data Encryption vs. Tokenization
https://www.centurybizsolutions.net/credit-card-data-encryption-vs-tokenization/

Century Business Solutions
Payment Card Tokenization
https://www.centurybizsolutions.net/payment-card-tokenization/

Century Business Solutions
How to Get PCI Certified
https://www.centurybizsolutions.net/how-to-get-pci-certified/

About Century Business Solutions

Century Business Solutions is reinventing the way companies accept credit card payments with their all-in-one payment solution, EBizCharge. EBizCharge is one of the top payment gateway alternatives and is specifically designed to reduce payment processing costs and inefficiencies. EBizCharge integrates seamlessly with over 50 accounting, ERP, CRM, and shopping cart systems, including QuickBooks, Sage, SAP B1, Microsoft Dynamics, Acumatica, Shopify, Magento, and WooCommerce. Century is partnered and certified with Microsoft Dynamics, Acumatica, SAP, Oracle, QuickBooks, WooCommerce, Magento, and many more.

For more information on Century Business Solutions, visit https://www.centurybizsolutions.com.