PCI Compliance for Law Firms: A Complete Guide

Written by Josh Kern

Today's clients look for the little things that make their lives easier. One of those things is paying for services online: 65% of legal clients prefer digital payments, such as credit cards.

The good news for lawyers is that law firms that give clients what they want also enjoy the benefits of convenience. In fact, 85% of law firms that accept credit cards get paid within a week of issuing an invoice, and 57% get their payment the same day.

Thanks to online payment processing solutions, it's never been easier for law firms to accept credit cards.

But accepting credit cards comes with its own set of ethics, regulations, and compliance responsibilities. Among others, you must practice payment card industry (PCI) compliance for law firms.

Check out our guide on law firm compliance, breaking down regulations from CLE, data privacy and security, financial regulations and more: Understanding Law Firm Compliance Requirements.

The rise of credit cards increases the need for law firm PCI compliance

Paper check payments saw a significant decline between 2003 and 2018, while debit and credit card payments grew by 6.8% per year from 2012 to 2015, then by 8.9% per year from 2015 to 2018. By late 2018, almost a third of US adults were exclusively using non-cash payments.

The growth of digital and contactless payments accelerated when the pandemic hit in 2020. Within a few weeks, almost 80% of people were using contactless payments. While some have returned to cash payments where possible, digital and contactless payments are here to stay.

If you simplify the logistics of doing business with you, more prospects will find your firm attractive. And they'll be able to pay you faster, too—provided you comply with law firm PCI regulations. As a result, accepting credit card payments makes your law firm more client-

centered and more aligned with current client expectations.

What is PCI compliance for law firms?

The Payment Card Industry Data Security Standard, more often written as PCI DSS, is a global set of security standards for handling credit card data. This standard helps companies keep the transfer of personal client data during credit card payments and the ensuing storage of any client data as safe as possible from hackers.

Do law firms need to be PCI compliant?

There is no specific set of PCI compliance standards for law firms, but PCI compliance is still a must if your law firm accepts or intends to accept credit cards.

For more information on law firm PCI compliance and other data security issues, check out our 2022 Law Firm Data Security Guide.

Why is PCI compliance important for lawyers?

When clients choose to pay you by credit card, they do it because it's convenient—and because they trust that the payment method is secure. Law firms and other businesses must earn that trust by taking the necessary steps to protect client data.

Data breaches can result in serious, long-term personal, business, and financial implications for clients. Lawyers who practice PCI compliance minimize this risk for their clients, as PCI compliance ensures that firms follow essential industry security guidelines.

These guidelines include maintaining a vulnerability management program, an information security policy, and advanced access control measures.

Does PCI compliance for law firms prevent cyberattacks and data breaches?

Although compliance with PCI standards significantly reduces the risk of a data breach for law firms, compliance does not guarantee data safety nor prevent consequences of a data breach.

However, lawyers that can prove their law firms' PCI compliance may be able to get their fines waived or reduced.

The importance of PCI Compliance for law firms

PCI compliance for law firms is critical—and beneficial—when accepting credit cards. Compliance enables you to offer your clients a more convenient, trustworthy, reliable, and safer billing option.

Law firm PCI compliance helps you avoid costly penalties

Large payment brands, including Mastercard, American Express, and Visa, take part in setting policies for PCI compliance for lawyers and other vendors.

According to the PCI SSC, if a law firm or other business fails to comply, it faces penalties provided by the relevant payment brands themselves.

Failure to practice PCI compliance for law firms may also mean breaking privacy and security laws, including the General Data Protection Regulation (GDPR).

Law firm PCI compliance reduces fraud

PCI compliance for lawyers, when done right, includes data encryption.

That means that, even if there's a cyberattack and hackers manage to get into your system, they won't be able to access identifying client information, such as credit card details.

As a result, they won't be able to impersonate cardholders, significantly reducing the repercussions of breaches.

Law firm PCI compliance provides a sales and retention differentiator

If you haven't joined the PCI compliance for law firms movement, you're not alone.

Non-compliance is a big challenge for companies across all industries. Only 52.5% of organizations across the world achieve 100% compliance. Only 39.7% of organizations in the Americas achieve the same.

PCI compliance can therefore become a business differentiator for client acquisition and retention, especially if you serve other companies. 65% of business buyers, or 73% if they represent an enterprise, considered the privacy and security measures a vendor takes before making a purchase.

When you accept credit card payments and practice PCI compliance, you offer clients something many companies, both inside and outside the legal industry, don't: Secure convenience that puts their needs first.

What are the requirements for law firm PCI compliance?

Vendors everywhere follow the same PCI guidelines and regulations, so law firm PCI compliance doesn't require reinventing the wheel. Experienced industry leaders have tested security practices repeatedly to verify clients are as protected as possible.

The PCI Security Standards Council has 12 requirements to guarantee PCI compliance for law firms and other companies:

- Protect cardholder data with firewalls.
- Change default passwords and other security aspects provided by suppliers.
- Safeguard the credit card information you store.
- Encrypt cardholder data.
- Keep your antivirus software updated.
- Secure all your systems.
- Restrict digital access to data about cardholders, even internally.
- Assign unique IDs to each computer user in your firm.
- Limit physical access to data about cardholders, even among your employees.
- Monitor every time cardholder data, or your network as a whole, is accessed.
- Continuously test system security.

To ensure your firm meets these requirements, you must educate your partners and firm staff, if applicable. The PCI SSC offers training and implementation support, making PCI compliance for law firms and other vendors easier.

What are the risks of non-compliance?

PCI compliance for lawyers is essential for your firm's and your client's security.

Non-compliance can lead to data breaches, which can lead to legal repercussions, fines, and client mistrust. All of which can have a significant negative impact on your bottom line.

Lawyers risk expensive lawsuits when they don't ensure PCI compliance for their law firms

PCI compliance reduces the risk of a potentially expensive lawsuit or settlement for compromised client privacy. Notable examples of costly data breaches include:

- TJX Companies offered a $40.9 million settlement to Visa customers impacted by a 2007 data breach.
- The Neiman Marcus Group paid $1.5 million due to a 2014 data breach, then announced another data breach in 2020.
- Capital One paid $80 million over a 2019 data breach.

Law firms pay fines when law firm PCI compliance fails

PCI compliance for lawyers doesn't just keep you out of court and away from expensive settlements. It also prevents heavy fines levied by payment card brands.

According to the American Bar Association, payment brands likely won't directly impose penalties on your law firm. Instead, they'll impose them on your bank. But the bank will pass the penalty on to your firm, leading to payments ranging from $5,000 to $500,000.

In addition, payment brands might decide to stop working with businesses not following PCI compliance guidelines, meaning you might not be able to accept Mastercard or Visa payments from your clients.

PCI non-compliance for lawyers results in reputation, trust, and revenue loss

Once a law firm's PCI compliance failure becomes public knowledge, trust and reputation loss tend to follow, leading to business loss.

Meanwhile, the costs of PCI non-compliance can continue piling up.

In 2017, Target settled a 2013 data breach with an $18.5 million payment, but that wasn't it's only financial loss: It also experienced a $440 million loss due to business expenses related to the breach, such as breach investigations and identity theft protection efforts.

PCI compliance is especially critical for small firms

Small and medium-sized businesses are often the most vulnerable to cyberattacks: More than 60% of cyberattacks target small and medium enterprises.

Smaller companies often don't have the resources to hire cybersecurity leaders, educate employees on best practices, or buy advanced technology. 47% don't even know how to protect their businesses and clients.

As a result, 60% of small businesses end up closing their doors within six months of an attack.

It's critical for solo lawyers and small firms to understand their compliance requirements, and to work with payment processing providers who offer PCI-compliant solutions.

How to ensure PCI compliance for lawyers

While some firms go through the process of ensuring PCI compliance for their lawyers, it's not worth the effort for most firms.

The more practical alternative is to use a PCI-compliant payment processing solution, especially one that specializes in legal payment processing and understands the unique challenges lawyers face.

The benefits of using a payment processing solution to provide PCI compliance for your lawyers

Just as PCI compliance is required when lawyers accept credit cards, every payment processing solution that accepts credit cards also needs to comply with PCI regulations.

The payment processing company goes through the entire process to create and maintain PCI compliance, so anyone who uses their services is also compliant.

Therefore, partnering with a dedicated payment processing provider makes PCI compliance for lawyers much more straightforward, while providing the same peace of mind for your firm and your clients.

When considering a payment processing solution provider, ensure they offer the following:

- Compliance certifications, including PCI and GDPR.
- Security experts to help law firms understand their requirements.

- Employee security protocols, including ongoing security training and limited access to sensitive data.
- Security vulnerability monitoring and appropriate patch codes.
- Data encryption for additional protection.
- Automatic backups of your account.

For more payment resources, be sure to take a look at our legal payments hub page.

Choose a payment processing solution that specialties in PCI compliance for lawyers

Although law firms have a lot in common with other service-based businesses, the legal industry has its own unique challenges, including ethical and regulatory considerations.

Choosing a payment processing solution that specializes in law firm PCI compliance, like Clio Payments, built into Clio Manage, helps you:

- Get premium chargeback protection for trust accounts.
- Comply with your state's ethics opinion on lawyers accepting credit cards (and know what to do if your state doesn't have one).
- Align with your state's rules about accepting advanced payments, charging fees, and other details specific to the legal industry and your state.
- Charge for billable hours or alternative billing arrangements, such as flat fees, subscriptions, and retainers.

PCI compliance for law firms is critical for a client-centered experience

Confusion or apprehension about security or PCI compliance requirements may contribute to law firms' slow adoption of credit cards.

But getting help from a solution that already ensures law firm PCI compliance when you process payments takes the worry off your shoulders. In turn, your firm can be one of the few that gives clients the convenience they want, combined with the data protection they need.

To learn more about PCI compliance and how to keep your law firm secure, be sure to read our 2022 Law Firm Data Security Guide.

About Clio

Clio is the global leader in legal AI, powering legal work across the profession, from law firms of every size to corporate legal teams, government agencies, and courts. Its Intelligent Legal Work Platform unites the business and practice of law, connecting the people, information, and processes behind legal work. Clio's AI brings the context together with legal sources drawn from Clio Library, a growing collection of more than one billion legal documents. Over 400,000 legal professionals in more than 130 countries rely on Clio to run their legal world. Learn more at www.clio.com.