Law Firm Security and Data Redundancy

LawPay®
AN AFFINIPAY SOLUTION

lawpay.com
866-376-0950

TABLE OF CONTENTS

At LawPay, Confidentiality, Privacy, & Security is Our Top Priority

Here at LawPay, we understand that you have an ethical obligation to maintain confidentiality. That's why keeping our customers' data secure is one of our top priorities. Managing privileged case information for thousands of attorneys (and their clients) is a responsibility we take very seriously.

We understand that some lawyers may be nervous about moving their data into the cloud. You undoubtedly have questions about the steps we take to ensure that your law firm's data is safe and secure, such as:

- What steps are being taken to protect my data?
- Does the company understand the unique concerns of lawyers?
- What will happen to my firm's data in the event of a natural disaster?
- How financially stable is the company that will be hosting my law firm's data?

In this guide, we'll answer all of these questions and provide an overview of the methods we used to ensure the security of your law firm's data. Our goal is to put your mind at ease by sharing our LawPay security procedures, which protect thousands of attorneys just like you.

What is Cloud Computing?

Cloud computing may sound like a new concept, but you're probably already using the technology in your law practice. The idea is simple: When you store sensitive client information online—whether in LawPay Classic, LawPay Pro, or a standalone online storage solution like Dropbox—you're storing information "in the cloud."

In other words, your data lives on servers owned and maintained by a third party, and your law firm can access files anywhere, anytime via an internet connection. Popular cloud tools include Westlaw, Google Drive, and online bank accounts.

Cloud computing offers many benefits, such as:

1. **Affordability**—Law firms can avoid costly solutions like in-house IT departments, expensive servers, and up-front infrastructure costs.
2. **Convenience and mobility**—Legal professionals can access their law firm's case files 24/7, from any location, using any Internet-enabled device.
3. **Security**—Cloud businesses, such as LawPay, can deliver exceptional data security for law firm and client information, and provide redundant data storage and backup.

A Brief Overview of LawPay's Security Procedures

AMAZON'S CLOUD COMPUTING PLATFORM

LawPay runs on an Amazon Web Service cloud computing platform. We chose this platform because of Amazon's experience managing cloud-based systems across four different geographical regions (16 U.S. availability zones) throughout the United States for some of the biggest companies and governmental organizations. Because of the breadth of Amazon's experience providing cloud computing services, you can trust them to be at the forefront of online service technology.

Amazon has strict procedures in place to protect the physical security of their servers and safeguard the integrity of their data. The company builds its data centers and network architecture to meet the requirements of the most security-sensitive organizations.

You can learn more about Amazon's cloud infrastructure and security at: http://aws.amazon.com/security/.

In addition to Amazon's security standards, we enforce network restrictions that ensure your data communications are never accessible to other AWS customers. We ensure confidential information is encrypted during transmission, whether between our own systems or external partners—including our payment providers and underwriting systems.

CONSISTENCY COUNTS

When it comes to protecting client data for your law firm, consistency counts.

LawPay's platform is regularly evaluated by independent auditors to ensure we meet specific service provider standards for Payment Card Industry Data Security Standard (PCI DSS) compliance. In addition, our internal and third-party security teams conduct consistent internal and external vulnerability scans to ensure the security of our payment solution.

We also constantly monitor the latest security threats, and evolve and adapt our service to address any issues that may arise.

ENCRYPTION

When you connect to our servers, your data is encrypted before transmission using 256-bit military-grade Transport Layer Security (TLS) connection. This is the same type of secure connection used in online banking, investments, and healthcare portals.

If your internet browser does not support full 256-bit encryption, the connection degrades to 128-bit, but by default your data is protected with encryption that meets state-mandated compliance standards. Our cipher suites also support Perfect Forward Secrecy (PFS) which prevents backward decryption of stored data should keys be compromised in the future. As a result, encrypting your transmission ensures that no unauthorized parties can access your data.

Protection in LawPay

In addition to the security steps Amazon and LawPay take on the server side, there are also a number of features built into LawPay that help keep your firm's data protected.

- LawPay will automatically log users out during times of inactivity or when the account has been accessed on another machine.
- LawPay uses best-in-class processes to safeguard your password and resist common attacks, providing your account with added protection. Our authentication systems are designed to be resilient against brute force attacks ensuring your account is only accessible to you.
- Features like Payment Pages and Card Vault prevent you from having to manually request and process client credit card information—minimizing your PCI compliance requirements. Your firm has its own PCI DSS compliance obligations, and LawPay takes measures to mitigate your law firm's cyber security risks. This includes displaying only the last four digits of a credit card number on receipts. As an additional service, LawPay has developed an easy-to-use PCI compliance program for our customers. You can complete the program yearly at no additional charge.

- LawPay tracks sessions and user activity to help monitor for suspicious behavior. To restrict access to sensitive information and enforce strong passwords, LawPay offers role-based permissions and password policies. Accounts are also protected by multi-factor authentication (MFA) and login safeguards.
- Under ABA Model rules, attorneys are responsible for selecting and implementing appropriate technology and procedures to safeguard client data. LawPay is built to ensure all payments are PCI compliant. We've also designed an easy-to-use PCI compliance program for our customers—free of charge.
- Built-in MFA for all users

You also have many different permission settings and access controls in LawPay that provide further protection. Permission settings allow you to control what each user can access within the LawPay platform, including staff, co-counsel, and clients.

TWO-FACTOR AUTHENTICATION

LawPay offers two-factor authentication, giving you an additional level of law firm security in the cloud. Two-factor authentication (or 2FA) is a security feature that makes it extremely difficult for unauthorized users to access your account. In the event that your username and password are compromised, 2FA would still prevent someone from gaining access to your confidential data.

Logging into a web-based software system that does not implement 2FA is a simple, one-step process. The user simply has to enter the correct username and password, at which point your data is made available.

Logging into a 2FA system, however, requires an additional login step. After users input a correct username and password combination, they aren't immediately logged into the system. A second step is required. The user will receive a time-based one-time password verification code which they must enter to complete the authentication process and gain access into their account.

What You Can Do to Protect Your Data

The most common cause of data loss is human error. That's why it's important to take steps to secure your account (in addition to setting up 2FA):

- Use a strong password. An app which manages and generates passwords (such as 1Password) is recommended.
- Don't use the same password for LawPay that you use for other websites.
- Use at least 10 characters and include a special character, number, and at least 1 capital letter.
- Don't give your LawPay password to anyone else, and generate strong, unique passwords for each site that are combined with 2FA.
- Make sure that other people can't access your email by implementing 2FA.

Should you ever feel that your account has been compromised, contact us right away! We can freeze access to your firm's account, immediately locking out all users until we can ensure that everything is secure.

We understand how important security is to your law firm. That's why we've built multiple security features into LawPay Classic and LawPay Pro. Our goal is to ensure that LawPay is reliable and your law firm data is protected and secure, so you can focus on doing what you do best: **practicing law.**

About LawPay

LawPay provides easy-to-use payments processing that takes the work out of getting paid. From sending payment requests and tracking transactions to protecting your IOLTA account, LawPay has you covered. LawPay Pro adds additional benefits to boost cash flow and productivity including invoicing, time and expense tracking, timesheet calendars, and advanced reporting. Learn more at lawpay.com.