Are you putting your clients' data at risk?

Is your firm doing everything possible to keep your clients' cardholder information secure? Is your payment processing environment secure enough to withstand hackers?

10 tips to keep cardholder data secure

Accepting credit cards means you get paid faster. But it also means you need to comply with PCI guidelines. PCI is short for Payment Card Industry Data Security Standard. It's the set of standards that manages how businesses accept credit cards and store card data — the two aspects of the payment process that are essential for protecting consumers' private data.

Review these 10 tips to make sure you're keeping your clients' data secure:

- Never write credit card numbers on paper or store them in unsecure programs, like Excel spreadsheets or Google sheets.
- Never use the default passwords for software or security systems.
- Install and regularly update the anti-virus software on your computer.
- Install and maintain a strong firewall.
- Limit and monitor employees' access to cardholder data — digital and physical.
- Assign a unique ID to each person at your firm who has computer access.

ClientPay

- Conduct training to ensure your team knows how to handle cardholder data securely.
- Encrypt cardholder data when it's stored or transmitted.
- Regularly test your security systems.
- Verify your payment processors are Level 1 PCI compliant.

Improve security and accounts receivable processes simultaneously

The right payment processing technology can help your firm save money on credit card processing fees, make your A/R processes faster, and keep cardholder data more secure.

To get all three benefits, look for a payment processing solution that offers security features that reduce your PCI scope. Examples of security features include:

- Automatically encrypting cardholder data
- Never storing cardholder data in your firms' walls, either physically or digitally
- Offering electronic wallets that support recurring payments but restrict visibility to card data
- Offering click-to-pay links that let your clients pay without making them create logins

Some payment processing solutions, like ClientPay, can integrate with your matter management software. This streamlines the steps involved in payment processing, and it reduces the likelihood of data entry errors.

How to convince your firm to invest in technology

You're convinced that you need to upgrade your firm's technology. But that doesn't necessarily mean everyone at your firm feels the same way. After all, we traditionally think of technology as being an investment — in both cost and time.

In reality, payment processing software doesn't need to interrupt your firm's work. Many teams save time and money when they change payment processing providers. And even more important than saving time and money? Keeping your clients' cardholder data secure. The right payment processing software can help keep your clients' data away from digital thieves.

Today, professional services are the third most-targeted victim of data breaches. And 50% of small businesses had data breaches in 2019. Your firm needs payment processing software and security processes to keep your firm out of those statistics.

As digital thieves get smarter, the responsibility of keeping data secure gets more important. It can feel daunting, but achieving PCI compliance is an essential step for firms that accept credit cards. Contact ClientPay to learn more about reducing your firm's PCI scope and streamlining your A/R processes.

ClientPay