PCI Compliance 101 | How to Protect Your Business

Jenny Houck & Griffin Dickerson

May 2026

Jenny Houck:

Hello, Griffin.

Griffin Dickerson:

Hello, how are you?

Jenny Houck:

We are here to talk about PCI compliance.

Griffin Dickerson:

Yes.

Jenny Houck:

Can you tell everybody a little bit about what it actually is?

Griffin Dickerson:

Absolutely. So PCI compliance is a framework that was put together by the PCI Standard Board. That includes Visa, a couple of other credit card companies, to just ensure that cardholder data is protected, properly used. And just secure within a payment card environment. When credit cards are processed, there's a lot that goes into that network wise, and there are various points along that process where that data could be exposed, and that could allow someone to take your credit card and steal all your money, so we don't want that.

Jenny Houck:

No, we don't. So how would I know if I'm okay? If I'm offering a credit card as a way of payment for my customers, how do I know that their data's going to be secure if I let them use a credit card or PayPal or Venmo? What do I need to do?

Griffin Dickerson:

Yeah, that's a good question. So I think there are a myriad of answers to that, and it really depends on how your organization is set up. I think if we're just taking credit card in hand and entering it into a computer, we want to make sure that that data is not being stored anywhere else, that we know who

has access to that data and who is typing it in, where they're entering that data, and then destroying it if it's physically printed afterward, or making sure that they're not, I guess, writing it down somewhere else.

Jenny Houck:

Well, if I have it written down because I don't have a software that encrypts it, can I lock it someplace or is that not good?

Griffin Dickerson:

Yeah. So I think first step would be to lock it somewhere. Not locking it is really risking someone coming in and taking it if it's not in a locked room, or at best, a locked cabinet. But I think further than that, when you're storing data like that in a paper form, in a printed form, you want to black out and sensor any of the actual credit card information. So you can keep names, you can keep individual background information, but last four digits of the credit card number, you usually want to hide those. And then the security code, expiration date, all of that, you don't want to store all of that information in one place.

Jenny Houck:

So are all credit card ... Are all payment methods equal in the sense of if I offer PayPal or if I offer the credit card or you can Venmo money, are those all the same?

Griffin Dickerson:

No. So there are different ways that those operate. Things like Venmo and PayPal are peer-to-peer payment services, so a lot of the encryption and card protection is tied to those individual services. So Venmo, they're responsible for hiding the credit card information. PayPal, same thing. Typically, when you're doing credit card payments, say at like a high school basketball game, folks often have a payment processor, something like Square or Stripe or I think Clover is another one, but those organizations will give you a card reader. I think Apple Pay has something similar as well with an iPhone, and that way, that data, they're processing the card in that instance. Someone can swipe their card. That data is not being stored by you, you're not handling it. Your organization doesn't have to worry about where that data is going.

So yeah, they're different and the same in that instance, but again, I think the biggest difference there and the biggest risk is when you're not using something like that, when you're not using a third party that typically is PCI compliant. So those organizations are rigorously audited to make sure that they are PCI compliant, and when you're storing it yourself, paper specifically is where the biggest risk is.

But I think to circle back to things like PayPal and Venmo, the risk that's posed there is on your end as far as who has access to those accounts, how often are we checking the transactions in those accounts, the limits in those accounts, what bank accounts are those accounts tied to, and where's that money going? Those are organizationally more of a concern, I think less so than the payment card.

Jenny Houck:

Now, there have been some changes lately in PCI compliance.

Griffin Dickerson:

Yes.

Jenny Houck:

Is that something that we should be worried about, or how do we make sure we're compliant?

Griffin Dickerson:

Yeah. So the big changes with version four came in March of 2025. Those had to be implemented at that date. Overall, just more of a focus on continuous security rather than point in time security. So understanding that the processes that we have in place that protect our environment are ongoing and not just done at the time for the audit, that they're consistently maintained throughout the year. Obviously with modern threats, more phishing, social engineering, AI being able to create a combination of attack vectors, PCI wanted to resecure those areas, and then that's where you see a little more of that continuous monitoring rather than a point in time.

Jenny Houck:

As you mentioned, when you come in for the audit, don't make it once a year.

Griffin Dickerson:

Yes.

Jenny Houck:

So what do I need to do to make sure? Because honestly, I'm only going to think about you once a year, and the audit's coming and what do I need to do? What should I be doing throughout the year that maybe I need to put on a checklist, part of my monthly close, quarterly? What do I need to do to make sure when you come in, I will have a clean audit and I'm protecting my customers?

Griffin Dickerson:

Yeah. So I think step one, like we mentioned before, censoring the sensitive information when you're storing it, if you're storing it. Preferably not, I would say. And then also regular access reviews is important. Making sure you-

Jenny Houck:

What do you mean by regular access review?

Griffin Dickerson:

Yes, good question. So regular access review consists of “where are we inputting the credit card data? Where are we receiving the credit card data? Who has access to that system where those things are stored?”

Jenny Houck:

So when you mentioned making sure that people have the right access, what do I need to look for to make sure the person basically maybe at my front counter is taking a payment, maybe they've written it down and then they put it in the system, or in the accounting department when they're doing reconciliations or getting reports, all the way to our IT department, what can they see and what can they do? What do I need to look for if I'm a manager?

Griffin Dickerson:

Right. Yeah. I think step one lies in the PCI standards themselves. There's something called an SAQ, a self assessment questionnaire that an organization can go through and fill out themself, and it details in a control form the things that need to be in place for an organization to remain secure around PCI. So I think that's step one, and you can either do that yourself or you can hire a third party to come in and take a look at that for you and make sure that you are compliant, perform some kind of gap analysis and show you where those holes might exist.

Jenny Houck:

So when you come in for the audit, what do I need to be prepared for? What should I expect?

Griffin Dickerson:

PCI as a framework as a whole is data security based, so I think again, I'd point back to the standard and say the security requirements in the standard are not super flexible, but depending on the organization, and there are variations to it that can give you some wiggle room tailored towards what your organization needs. But I would start looking at those, looking at the types of SAQs or self-assessment questionnaires and determining where you fit in there, and then applying that to your organization.

Jenny Houck:

So for that self-assessment questionnaire, is that something that I reach out to Barnes Dennig and they have it? Should I find it someplace at pcicompliance.com? How do I find what that is?

Griffin Dickerson:

Good question, yeah. The latter, for sure. PCI, if you just look up the PCI standard, our website has a full document resource library. You can download any of the SAQs from there, and they have explanations as well. There's an SAQ guide that you can download as well that will show you, "Hey, if your

organization operates in this fashion, this is the best SAQ for you. These are the things you need to be concerned about."

Jenny Houck:

Now, would you be able to tell us, if we are not compliant, what are the ramifications? If I have credit card data that I'm writing out, I'm not blacking this stuff out and someone comes in and takes it and uses it, are there consequences to me or is that just, there's fraud for somebody and they have to deal with it?

Griffin Dickerson:

Yeah, so a little bit of both. I think obviously, the individual has to deal with it, but I think one of the biggest things that can harm an organization is just trust. Your customer base suddenly no longer trusts that you're properly handling their data and that's putting them at risk. So whether or not that legally can fall back on you, even if it doesn't in that circumstance, the trust of your customer base is lost, and those reputational consequences for sure.

Jenny Houck:

What do executives and leaders within an organization need to do to be compliant?

Griffin Dickerson:

So compliance overall should be treated as more of a governance and enterprise risk issue, not just a technical issue. The IT folks obviously and cybersecurity folks obviously have a hand in ensuring that the environment is secure and that the data is properly protected, but ultimately, it falls on the entire organization reputationally and so on. So I would say that's where you start, and then I think gaps in compliance can quickly turn into some audit findings, reputational damage and potential penalties. Depending on the credit card processors that you all are working with, it oftentimes can turn into financial penalties in that area as well.

And then lastly, I would just say I think when leadership looks at it in that manner, that it is an overall business risk, it becomes a lot easier to identify those gaps and find a reason to put time and effort into remediating them.