by Bill Gogel

6 Questions Answered:

What Municipalities Need To Know About PCI Compliance

Card payment fraud has evolved a lot over the years, but as municipalities are finding themselves a target for hackers, they are asking how they can protect themselves from a data breach. Hackers are typically out for financial gain, so credit card compromise can be a lucrative business for them. PCI compliance can help protect against those breaches and potential financial and reputational loss.

What Is PCI Compliance?

Before 2004, each card brand, Visa, Mastercard, American Express and Discover, all had their own credit card security program that each business in the card payment ecosystem had to follow. As you can guess, this was difficult for businesses to juggle each card brands' expectations, and at times these security standards were difficult to line up among the card brands.

In 2004, the card brands came together and formed the Payment Card Industry (PCI) Security Standards Council (SSC) that unified the security requirements (Data Security Standards or DSS) for merchants and service providers. This Council was tasked with developing the standards with participating organizations such as retailers, payment processors, banks and security experts.

As payment fraud began to rise, it became within the card brands' best interests to increase credit card security while balancing the ease of use for customers and merchants. Seventeen years and nine revisions to the standard later, we have a mature security framework for capturing, issuing and processing card payments.

Who Needs To Comply With PCI?

Just about every municipality collects credit and debit payments:

- Parks and Recreation
- Vital Records
- Permits
- Tickets/Violations
- Taxes
- Reservations
- Utilities

If you do, there is a certain level of PCI compliance that you must maintain. Understanding what those levels are can be confusing for municipalities that have several payment vendors and payment channels.

But what if you outsource these payment functions? The truth is that most merchants outsource some or all of their payment processing to a third-party service provider. This route can significantly reduce your PCI compliance efforts as you have outsourced the responsibility of cardholder security. It is important to note, that even though you have outsourced the responsibility, you cannot outsource the accountability. If a credit card data compromise happens to your customers, you are still on the hook for any fines or penalties.

If you process less than 6 million card transactions annually, you can likely qualify for a self-assessment and may not need to hire an outside security expert. A self-assessment questionnaire usually comes at the request from your acquirer, the bank or payment processor you have contracted with; also known as the merchant bank. Acquirers are responsible for making sure you are PCI compliant, since they share the risk of a credit card data breach. Generally, the more annual transactions you capture, the more scrutiny your acquirer is going to apply.

There are nine different types of questionnaires, which one is right for me? This is the tricky part, and the short answer is that you may want to consult with your acquirer or with an outside PCI consultant. Since your acquirer knows how you take payments, they can provide guidance on the right questionnaire. Knowing which questionnaire means you can answer anywhere between 24 and 283 questions – so not doing more than you need to can be a huge time and effort savings. Generally, the type of questionnaire depends on how you accept card payments:

- "Card-present" that are in-person swipe/dip/tap payments
- "Card-not-present" that can be online, mail-in and telephone payments

If you have multiple acquirers, then you may want to get outside help from a Qualified Security Assessor (QSA).

Who Can Help With Compliance?

There are a lot of great security experts and consultants that can help in this area, but the PCI SSC has a registry of assessors that specialize in helping companies understand PCI requirements, help reduce PCI efforts, and perform assessments. You can find a list of assessors on the PCI SSC website under "Qualified Security Assessors." Visit https://www.pcisecuritystandards.org/.

What Are The Non-Compliance Risks?

Non-compliance risks are largely financial and reputational. Let us take a real-life example and study the outcome of a cardholder data breach.

In 2013, Schnucks, a regional grocer with nearly 100 stores, suffered a cardholder data breach that affected approximately 2.4 million customers. This made headlines over several months as customers reported fraudulent activity, fingers were pointed and litigation ensued.

The key players in this case were First Data Merchant Services (Schnuck's acquirer) and Citicorp (FDMS's funding bank). The acquirer is the first party that assumes the burden of reimbursing cardholders and issuing banks, covering additional losses, and paying for identity theft monitoring. The acquirer is entitled to pass on these losses to the merchant if they determine they were at fault for the data breach.

Luckily for Schnucks, the aster Service Agreement (MSA) limited the grocer's data breach losses to $500,000 per incident. While the total financial impact was never published, it is very likely that the losses significantly exceeded the $500,000 cap. This went into litigation that also resulted in legal costs. And finally, the grocer came under intense scrutiny by the card brands and acquirer to enhance their PCI compliance program that likely resulted in significant costs.

There are a lot of facts not mentioned about this case, but it exemplifies how a data breach can have financial and reputational consequences.

What Are Common Requirements?

As a QSA, this is where I spend most of my time with clients: helping them understand the requirements, giving implementation guidance, and helping them develop a sustainable compliance program.

Depending on how you take card payments, you may only have to comply with as little as 24 requirements, or as many as 283 requirements. From the assessments that we have performed, these are the most common security controls:

- Having an up-to-date Information Security Policy
- Having an up-to data Incident Response Plan
- Maintaining a vendor management program to ensure your vendors are PCI compliant
- Scanning quarterly for internal and public system vulnerabilities
- Securing network configurations to minimize the risk of a breach
- Limiting access to cardholder data
- Using and updating anti-virus and anti-malware software on commonly affected devices

What Other Questions Should I Be Asking?

Is IT involved in an annual self-assessment? Often times a finance or treasury function maintains the relationship with the acquirer, and that function is the first person that may receive a self-assessment questionnaire from the acquirer. In my years of helping clients with PCI compliance, sometimes these very technical questionnaires never cross an IT's desk. Make sure your IT is involved going forward.

Are we storing cardholder data? Not storing cardholder data can significantly reduce your PCI compliance effort. Think about how you might store it in both electronic and physical formats. Common areas where cardholder data might be hiding are:

- Email
- Filing cabinets
- Spreadsheets
- File shares

Do we use secure technologies such as Point-to-Point Encryption (P2PE) for card-present transactions? This newer technology is a great way to secure card-present transactions while also requiring a very minimal PCI compliance program. If you are not using P2PE payment terminals, you may want to ask your acquirer about it.

Do we host or manage any online payment pages ourselves? If you have not completely outsourced your e-commerce payments, then you may be exposing vulnerable websites to the internet. There is a whole set of PCI requirements that have to be audited if you host your own payment page, and it is best to outsource that if possible.

What is something that I can do right away to reduce my risk? The PCI requirements prohibit you from storing the security code (the 3- or 4-digit code) after you have processed a payment. Sometimes these codes are stored long-term on a physical form in a filing cabinet. You can audit those physical files and destroy/obfuscate those codes to come back into compliance and greatly reduce your risk. While you are rummaging through filing cabinets, you may also want to rethink whether you really need to store those physical forms at all.

Key Takeaways

- If you take credit card payments, you are subject to PCI compliance requirements.
- You can outsource credit card processing to reduce your PCI burden.
- Engage a QSA if you need professional help in shaping your PCI compliance program.

Bill Gogel *is senior manager, risk assurance and advisory at Armanino. He provides IT and cybersecurity consulting services, drawing upon his expertise to help organizations assess their cybersecurity posture, develop cybersecurity roadmaps and communicate cyber challenges and solutions to their leadership teams. He works within a wide array of security frameworks, such as: MITRE ATT&CK, NIST Cybersecurity Framework (CSF), CIS Critical Security Controls, PCI DSS, SOC 1 and 2, NIST 800-53, COBIT, COSO, ISO IEC 27001/ISO 27002, NY DFS, GDPR and HIPAA/HITECH.*

Bill manages Armanino's ethical hacking team, that provides penetration testing, vulnerability assessments and social engineering exercises. He holds the designations of Certified Information Systems Security Professional (CISSP), Qualified Security Assessor (QSA), and Certified Information Systems Auditor (CISA).