ONE INC

PCI: What it Means to Your Insurance Company

What is PCI?

PCI DSS (Payment Card Industry Data Security Standard) is a set of standards that guarantees the security of credit card processing. These standards apply to companies that accept, process, store, or transmit credit card information. The PCI standards are managed by the major credit card companies, including Visa and MasterCard.

Why you should care about PCI Compliance

As soon as you accept credit cards, you must be PCI compliant. There are multiple levels of compliance that can apply. Depending on which applies, your burden to demonstrate compliance can vary immensely. That burden is determined by what PCI calls a Self-Assessment Questionnaire (SAQ). Levels range from the least burdensome, which is SAQ A, to the most, which is SAQ D.

If, for example, you are storing electronic cardholder data on your own systems, you will likely be a level SAQ D. The requirements for PCI compliance at this level are extreme, requiring multiple extensive audits per year, and initial systems costs that can run into millions of dollars and require constant maintenance.

Being out of compliance is not really an option for an insurance company, as PCI compliance penalties are severe. In addition to fines that can be up to $100,000 per month, your bank may also terminate your service. Companies have gone out of business because of PCI compliance violations.

Storing credit cards - the big risk vs. the big benefit

Accepting credit cards is more than just a requirement for acquiring a new customer. It's also important for customer retention. Keeping a credit card number on file for a customer makes it that much easier for a policyholder to renew their policy.

Unfortunately, this is where exposure is greatest and why the PCI compliance requirements are so stringent at this level. Storing credit card data improperly is an invitation for hackers and security issues. However, in this competitive market, choosing not to store credit card information just so you can meet lower PCI compliance requirements is not a viable solution.

ONE INC

PCI: What it Means to Your Insurance Company

The solution

What is the best strategy to reduce the scope of your PCI exposure and burden? You can effectively "outsource" the acceptance and processing of credit cards to a vendor whose business is to understand and stay on top of managing PCI compliance. These vendors provide for the storage of credit card data, but not on your systems. That means you can typically be classified at a PCI level of SAQ A, which requires none of the costs and other resources associated with audits and other measures required to meet compliance requirements of higher levels. Because the vendor undertakes all these measures, you do little more than file a simple self-attestation of compliance.

Especially for recurring payments, a third-party processor is absolutely the best route. The most reputable and highly-certified vendors will use vault and tokenization technology. This strategy means the credit card number is never in your possession—you don't see or store the number—ever. With tokenization, the payment processor never stores credit card numbers, either. The processor, instead, passes the card information along to the credit card company, which then issues a token valid for that, and future, transactions. Even if a hacker manages to insert himself into the flow of information, the most he can get is a token which is worthless outside the context of the policy purchase.

PCI standards are constantly changing. Choosing a payments provider that is both conversant with the needs of the insurance industry and deeply experienced with PCI provides ongoing benefits. You can invest significant resources and take on great risk to do this on your own or you can use a vendor for whom payments processing is a central part of their business.

A final word

When looking for a payment processor, make sure you select one that is PCI DSS Level 1 certified. Vendors achieving this highest level of certification must undergo an extensive multi-month external audit annually. You get the PCI scope reduction you need—and keep it, both over time and as your needs expand. With a vendor at this level of certification, you can offer whatever credit card capabilities your business demands.

To learn more, contact One Inc at sales@oneincsystems.com