

Getting to Market Faster by Outsourcing PCI Compliance

Peter Berg, VP of Business Development & Strategy, Very Good Security (VGS)

Brian Whorley, Founder & CEO, Paytient

WEBINAR SUMMARY

KEY TAKEAWAYS

- Build in regulatory compliance and security before it becomes a problem.
- Key checkpoints along the way help bring a compliant product to market.
- Outsourcing PCI compliance to a trusted partner can decrease costs.



OVERVIEW

Building a payment card industry (PCI)-compliant cardholder data environment is a time-consuming and costly project that often delays critical time-to-market timelines more than many organizations can afford, especially startups.

Outsourcing compliance, including PCI compliance, and security to a knowledgeable partner like Very Good Security can help businesses get to market faster and decrease the direct and hidden costs associated with PCI compliance.

CONTEXT

Paytient, a payment card provider whose mission is to eliminate cost as a barrier to healthcare, operates at the intersection of financial services and healthcare. Brian Whorley and Peter Berg discussed how compliance and security partner Very Good Security helps Paytient and other vendors meet compliance requirements.

KEY TAKEAWAYS

Build in regulatory compliance and security before it becomes a problem.

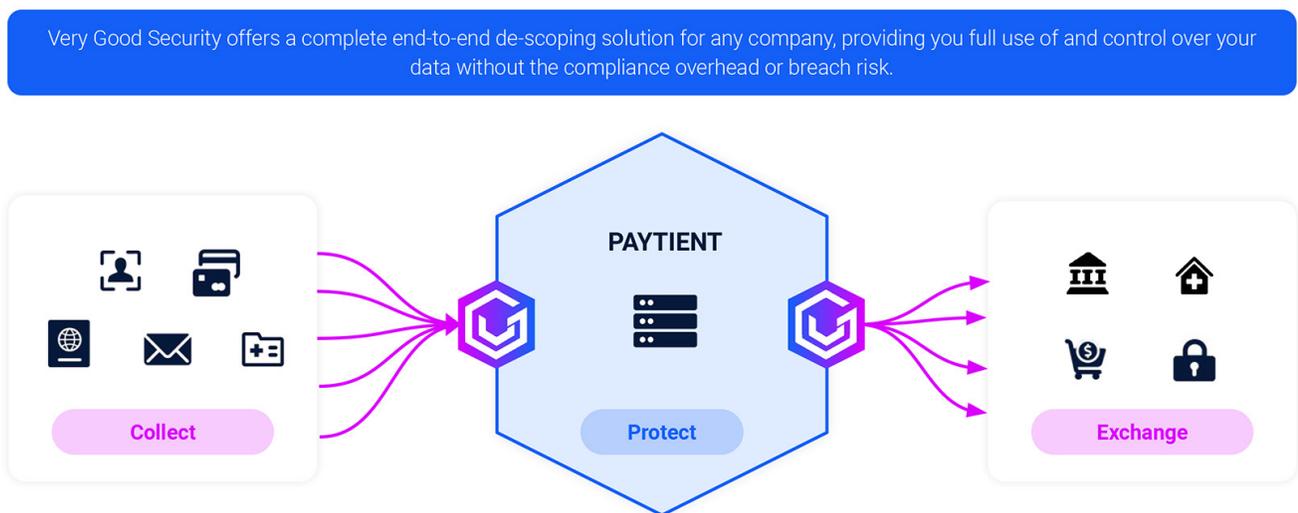
Paytient built regulatory compliance and security into its product as it was being developed, attacking the (potential) problem before it became an actual problem. This allowed the company to build in the features it needed while letting Very Good Security focus on the compliance and security aspect.

Companies working with PCI compliance and other regulatory or security requirements need to build in these pieces as early as possible. Shifting the burden of compliance and security to a knowledgeable and trusted partner, like Very Good Security, allows companies to focus on their core competencies and move quickly to market while reducing risk and the scope of regulation or compliance burdens.

We've seen customers twist themselves into pretzels trying to avoid regulatory and security issues. They end up clipping their own wings, limiting what they're able to build.

Peter Berg, Very Good Security

Figure 2: Very Good Security helps Paytient separate the business logic from data security



Key checkpoints along the way help bring a compliant product to market.

When building in PCI and other regulatory compliance and security into a product, there are several key checkpoints along the way that can help companies ensure they are efficiently and effectively meeting the requirements.

Key checkpoints when bringing a compliant product to market

- | | |
|-------------------------|--|
| 1. Define the end goal | Determine the intended outcome of the product and identify what tasks and components are necessary to achieve that end goal. |
| 2. Reduce scope | Reducing scope limits risk. For compliance and security, this applies to focusing on the actual information that needs to be collected and handled; don't capture large amounts of data that won't be used. |
| 3. Evaluate the options | <ul style="list-style-type: none">– Consider the different options available for compliance and security.– Understand the hidden costs associated with the end goal.– Evaluate vendors and partners with care to ensure the best and right solution is selected and that it meets the product's needs. |

Outsourcing PCI compliance to a trusted partner can decrease costs.

The average cost associated with developing a PCI-compliant solution is \$1 million, although that number can be even higher in more complex environments and lower in very simple environments. Depending on the scope of the project, the cost can also decrease significantly when working with a trusted partner.

Figure 3: The real cost of PCI: Approximately \$1 million



*Based on previous customer implementations for PCI compliance. Exact savings depend upon integration complexity.

Working with a trusted partner also allows organizations to offload the “pain” associated with PCI compliance to an expert in the field. In addition to reducing the PCI pain, an expert can also impact costs.

A company facing PCI on its own needs to not only develop the solution, but go through the auditing steps associated with proving that the product is PCI compliant. This can include stepping back and fixing issues identified during the audit, before going through a subsequent audit. This entire process can take six months to a year. The audit also needs to be handled annually.

A partner like Very Good Security takes on all of the compliance and security overhead, freeing up an organization's developers to work on competitive product features, rather than having to focus on maintaining the PCI environment, fixing associated bugs, and preparing for and participating in annual audits.

The outcomes that get me excited are when customers are doing new and innovative things they were unable to do [before Very Good Security].

Peter Berg, Very Good Security

Berg shared an example of the very first PCI level one customer that Very Good Security worked with. This company wanted to get to market within six months, yet PCI compliance was normally a 9- to 12-month process. Very Good Security was able to ensure compliance and go through the PCI audit in less than one month, allowing the company to make its timeline goal.

BIOGRAPHIES

Peter Berg

VP of Business Development & Strategy, Very Good Security (VGS)

Peter joined VGS from Visa, where he created and led Visa Ventures, their global venture investment arm responsible for investments in early-stage payment and technology companies including Stripe, Marqeta, Klarna, Chain and more. Before leading Visa Ventures, Peter helped shape Visa's product strategy in new and emerging payments, and lead Visa's relationship with Square. Prior to Visa, Peter was a co-founder or early employee of several successful startups in financial services and technology; two were acquired and one remains privately held today.

Brian Whorley

Founder & CEO, Paytient

Brian is the CEO of Paytient – which you can think of as a line of credit for medical expenses. This is the second time he has started a successful company, and this latest startup is doing something innovative to help employees assume greater financial responsibility for their healthcare. Before starting Paytient, he spent a few years at a community hospital in Columbia, Missouri.