zilch

Case Study

Client

Zilch is a ubiquitous BNPL payment platform company with a disruptive direct-to-consumer approach that lets users pay anywhere that accepts Mastercard via tap & pay, in-store, online or offline at over 37m locations. Valued at $2Bn, they reached 2m customers in 18 months (just in the UK) faster than any other fintech and today they have close to 40K reviews on TrustPilot and an impressive 4.7 rating.

Sean Hederman, CIO

Region

Global

Industries

BNPL, Payments, Fintech

Goal

Become PCI Level 1 certified and maintain a 'zero data' network.

Challenge

Upgrade PCI compliance from Level 3 to Level 1. Prevent customer card data from ever touching the in-house network.

Solution

VGS Control for PCI DSS Level 1 Certification and VGS Vault for Data Security.

Result

Eliminated card data environment (CDE); Upgraded to PCI Level 1 compliance at least 3x faster than they could have in-house.

Background

Sean Hederman, CIO of Zilch, believes "the best kind of information, the most secure kind of information is the information you don't store it all." Luckily, as one of the first hires at the company – and acting chief architect and chief information security officer – he's been in a position to make sure Zilch never stored sensitive customer data.

But for a long time, card information was transiting their system. Though Zilch's card data environment (CDE) and extensive security controls kept customers safe, it was always in the back of Sean's mind that there must be an even better way. The need to achieve PCI Level 1 compliance sparked a search that would lead them to the solution.

Challenge

Protecting customers' sensitive data – their debit card information, Zilch card details, and social security numbers (in the US) – is critical to Zilch's success. With a fully built out card data environment (CDE) and a relatively sophisticated security control program in place, the team had achieved PCI Level 3 compliance to keep that card information safe.

But in their growth and their efforts to continually improve security, Zilch decided to upgrade its compliance to PCI DSS Level 1. Even with their existing compliance infrastructure, Sean says, "We knew that it was going to be hugely onerous on us. It was going to take six months to get everything set up for the [PCI DSS] audit, and it's going to be a huge distraction, which we didn't really want to have. So, we started looking for options around who could hold our hands. That's how I came across VGS."

VGS also happened to solve another challenge that had nagged for some time: keeping sensitive data from ever touching Zilch's environment. As it was, Zilch was collecting debit card information from customers and passing it out to their acquiring partner. The acquiring partner would then exchange the card number for a token. The problem? Data touched the Zilch network before being passed to their acquiring third party, which left it vulnerable. And as Sean puts it, "We don't want to take any risk."

> *"We knew that it was going to be hugely onerous on us. Meaning it was going to take six months to get everything set up for the [PCI DSS] audit, and it's going to be a huge distraction, which we didn't really want."*
>
> Sean Hederman, CIO

Solution

From the very first look, Sean was impressed with the VGS solution technically. "It's a very elegant solution. With just a quick configuration on our side, payment card information essentially hops over our entire company."

No More CDE and An Easy Hop to PCI Level 1

Now that payment information no longer touches Zilch's networks, the card data environment they painstakingly set up and maintained became obsolete. The team got rid of their CDE but kept most of the security controls they'd put in place to continue their industry-leading security program. Sean says, "We've now gotten rid of our cardholder data environment since card numbers no longer touch our network. More importantly, we now know that even in a complete breach scenario, hackers would not get access to that card information because we simply don't have it."

This change to Zilch's architecture helped "immensely because essentially most of our systems were now out of scope," shares Sean. And since they already applied PCI controls to most of their network, by adding VGS's expertise, upgrading to level 1 wasn't a huge lift. "PCI level one is a much more rigorous standard – but it wasn't a gigantic exercise. We did the whole PCI compliance, including changing policies and the audit, in about two months." VGS also introduced the team to an auditor, something Sean says was beneficial.

Proactive Compliance for Global Expansion

During the audit process, the Zilch team used the VGS Control dashboard. As they expand across the globe, they're finding the dashboard extremely helpful in getting compliance information proactively prepared for each new country.

"We found [the Control dashboard] really, really useful. It's very well organized, and the information required for the auditors is universal. Now that we're expanding into so many new countries, we're using the Control panel as inspiration. We take the pack of information as a preliminary POC and provide it to third parties and banks when we begin engaging with them."

New Countries, New Use Cases

And as Zilch expands to new countries, the team discovers new use cases that VGS solves for them too. For example, in the United States, it needs to collect Social Security numbers to pass to back-end systems for things like credit checks. Luckily, VGS Vault takes care of this super sensitive PII data just as well as it does payment card information.

> *"[With VGS] we know that even in a complete breach scenario, hackers would not get access to that card information because we simply don't have it."*
>
> Sean Hederman, CIO

Results

In the end, Sean says VGS is how Zilch ensures customer information stays safe. "VGS is a fantastic way of ensuring that that card information not only arrives at the required destination but does so in a way that we are absolutely sure we cannot lose it." And by keeping that data safe, they've been able to eliminate their card data environment, which reduces complexity and increases overall agility. This also allowed them to build their US environment in less than a third of the time it took to build the U.K. environment, a significant accomplishment.

And at the same time, as they lightened their technical load, they were able to upgrade their PCI compliance from Level 3 to Level 1 – at least 3x quicker than they would have been able to on their own. Sean shares, "Our [PCI Level 1] timeline went from this huge six-month project with tons and tons of audit prep to this much lighter lift, one to two-month project with VGS."

> *"Our [PCI Level 1] timeline went from this huge six-month project with tons and tons of audit prep to this much lighter lift, one to two-month project with VGS."*
>
> Sean Hederman, CIO