COALFIRE

CASE STUDY

Qualpay chooses Coalfire to validate security and achieve PCI DSS compliance to maximize market adoption

AT A GLANCE

For Qualpay, achieving the Payment Card Industry Data Security Standards (PCI DSS) Report on Compliance (ROC) in a timely manner was critical to maintaining business. As an industry leader, the processor knew it needed an experienced expert to efficiently assess and validate its PCI DSS efforts while protecting the security of its payment platform.

CHALLENGE

For payment processors to provide processing services, PCI DSS compliance is required. As a leading provider of integrated, omnichannel payment solutions, Qualpay wanted to not only achieve PCI compliance, but also make certain its cloud-based payment platform was secure. However, a security-first approach couldn't put its deadline at risk or overburden its internal resources.

When its previous Qualified Security Assessor (QSA) firm replaced personnel mid-engagement and travel expenses grew too high, the processing company knew it needed an experienced QSA firm with cloud expertise that would assign a senior-level assessor for the entire engagement. Qualpay needed a trusted cybersecurity partner who could provide support as its infrastructure and environment evolved.

"Our previous vendor was based in Atlanta, which meant that travel expenses for onsite visits were quite high," explained Qualpay's CIO. "During our short engagement with that vendor, our original assessor left the company, leaving us in the care of a more junior member. The assessor we worked with knew the PCI DSS requirements quite well, but clearly was inexperienced in performing assessments with customers and lacked necessary cloud knowledge."

The CIO had partnered with Coalfire at a previous employer and recommended Coalfire to the organization's executive leadership team. "Coalfire's experience assessing companies using cloud infrastructure, such as Amazon Web Services (AWS), was just one of the many reasons we chose to partner with Coalfire for our PCI DSS ROC," said the CIO.

APPROACH

As the go-to advisor on cybersecurity and compliance, Coalfire leveraged its PASS+R methodology, years of experience, and deep

technical expertise with PCI DSS requirements and cloud services to assess and validate the organization's environment against the rigorous standard.

Coalfire started the engagement with:

- **Pre-assessment and analysis:** Coalfire conducted a project charter call to determine timelines, resource allocations, and scheduling to prepare for the PCI DSS onsite assessment. Coalfire introduced Qualpay to the secure, powerful CoalfireOne℠ platform as a means to gather, retain, and review evidence in accordance with PCI DSS standards. The CIO and his team uploaded high-level system and business information, allowing Coalfire to examine the organization's cardholder data environment in its entirety and efficiently move to the onsite phase.
- **Sampling and testing:** Coalfire performed a comprehensive onsite assessment at Qualpay's Bay Area headquarters. Coalfire visited the organization's office and conducted a physical walkthrough of the facility. As a final task, Coalfire and Qualpay conducted configuration checks on system components, including network devices and servers located within the payment processor's production facility hosted on AWS.
- **Remediation and submission:** After the onsite visit, Coalfire prepared a remediation action item list (RAIL) that identified data requests and required remediation for a successful revalidation of PCI DSS compliance. By leveraging CoalfireOne's task assignments, dashboards, document management, and tracking features, the combined team efficiently and easily resolved the RAIL requirements. As a result, Coalfire validated Qualpay's remediation efforts and prepared a ROC.

"I have been impressed by the breadth of knowledge that Coalfire's assessors have shown regarding PCI DSS requirements, and how they apply to our environment. The assessors not only know the requirements in detail but can readily speak to how implementation of particular processes and methodologies in our cloud-based environment satisfy those requirements."

– QUALPAY'S CIO

CS_QualPay_120517

RESULTS

With extensive PCI experience and a team of highly skilled assessors, Coalfire has served as Qualpay's partner, helping the company reduce business risks and achieve compliance as it innovated its platform, business, and technologies over the past three years. "Coalfire has helped us remain PCI complaint in the cloud as we have continued to innovate our payments platform and grow our business," explains the CIO at Qualpay.

"We must remain PCI-compliant each year to continue doing business in our industry. Achieving this compliance is a complex effort, requiring many disparate types of evidence and policies. Coalfire does an excellent job every year by efficiently walking us through the requirements one by one so we're confident in the security of our platform and don't put our compliance validation at risk."

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 16 years and has offices throughout the United States and Europe. **Coalfire.com**

COALFIRE.