TEVORA™

Case Study

Tevora's PCI DSS Compliance Services—A Steady Hand in Turbulent Times

In the best of times, maintaining compliance with the complex and evolving Payment Card Industry Data Security Standard (PCI DSS) is a challenge. But when organizations face challenges such as the Covid pandemic, entering new businesses and markets, or selling lines of business, the degree of difficulty increases exponentially.

Fortunately, Tevora's experienced team of payment security experts can help organizations maintain PCI DSS compliance in even the most turbulent of times.

We have been a certified PCI Qualified Services Assessor (QSA) since the PCI DSS standard was created in 2004. And we've helped some of the world's leading payment companies stay compliant with PCI DSS as they have experienced significant changes in their business and technical environments, including strategic pivots, the addition of new business lines, migration to the cloud, ransomware attacks, and natural disasters to name a few.

In this case study, we'll describe how Tevora helped a leading global financial services company maintain PCI DSS compliance as it navigated significant changes. To protect our client's confidentiality, we'll refer to them by the fictitious name of Global Financial Services (GFS).

Off to a Great Start

Tevora began working with GFS six years ago to help them bring their peer-to-peer money transfer service into compliance with PCI DSS. After doing this, we performed a service assessment to validate their compliance with PCI DSS Level 1 requirements and documented the successful validation results in a Report on Compliance (ROC) and Attestation of Compliance (AOC).

We completed this first project on time and within budget, and GFS management was delighted with the results.

Building on Success

Based on the success of our first project, GFS asked us to conduct annual assessments of their peer-to-peer money transfer service to validate ongoing compliance as their service features and PCI DSS requirements evolved.

Over the last five years, Tevora has continued to deepen and expand its relationship with GFS and currently performs annual PCI DSS service assessments for the following services:

Global peer-to-peer money transfer service

Level 1 validation results are captured in ROC and AOC documents.

Cloud-based e-commerce payment gateway service

Offered to GFS clients in Europe. For this service, we help GFS prepare a Self-Assessment Questionnaire (SAQ) to validate compliance.

Global bank-to-bank money transfer service

Level 2 validation results are captured in an SAQ document.

Global card payment service

For this service, we help GFS prepare an SAQ to validate compliance.

To date, we have partnered with GFS to deliver all annual PCI DSS compliance projects for these services on time and within budget. And the fact that none of the services has experienced a significant data breach speaks to the quality and thoroughness of their PCI DSS compliance.

Tevora's Proven PCI DSS Compliance Methodology

For our work with GFS, we use Tevora's proven three-step compliance methodology that has been honed and refined as we've helped our clients achieve PCI DSS compliance over the years. It uses a simple, cost-effective approach to guide clients through the compliance process. Here's a summary of the methodology:

PCI DSS Compliance Methodology

Process Step	Description
1. Gap Analysis	• We start by doing a **detailed review of your environment,** including systems, security controls, policies, and other security documentation, to identify areas where improvements are needed to meet PCI DSS requirements. • Our payments experts work with your team to outline **strategies for a cost-effective road to compliance.** • We help define a **scope for your compliance effort** that covers all of the needed work but prevents you from wasting time and money pursuing low-value activities. • Our experienced QSAs **assess and validate security controls** early in the process, ensuring remediation efforts are directed and focused.
2. Remediation	• We **partner with your team** to perform as much or as little of the remediation work as you'd like. • Remediation work may range from writing or modifying **security policies to implementing security controls or technical solutions.** • Our QSAs provide **advisory services to the team** implementing remediation solutions to ensure the end result will align with PCI DSS requirements.
3. Certification	• As your trusted advisor, Tevora ensures your ROC, AOC, SAQ, and other required **reporting is executed in confidence and on time.**

Overcoming Challenges

To achieve our outstanding level of success in partnering with GFS over the last six years, we've had to get creative and work smart to overcome some significant challenges.

Responding to the Pandemic

In early 2020, when the Covid pandemic began significantly impacting life in the United States, Tevora's team was working onsite at GFS offices to conduct the annual PCI DSS assessment of their peer-to-peer money transfer service.

In March 2020, GFS transitioned to remote-work-only in response to the pandemic. This required Tevora, working in partnership with GFS, to perform some rapid planning and intensive work to develop a plan for completing the assessment while working remotely. Fortunately, the team was able to complete all necessary onsite work and ensure online access to documentation prior to transitioning to remote work, which enabled the remainder of the project to be completely remotely.

Thanks to our deep partnership with and GFS, creative planning, and some focused extra effort by both Tevora and GFS staff, we were able to complete the PCI DSS assessment on time and within budget, maintaining Tevora's perfect record of project delivery at GFS.

Pivoting To Support Sale of a Service

While not mentioned above, GFS had also engaged Tevora to conduct annual PCI DSS compliance assessments for their bill pay service, which ran in a legacy data center environment. We performed these assessments successfully for several years until GFS decided to sell the service to another company, which we'll refer to here as "Global Integrated Financial" (GIF).

After purchasing the bill pay services from GFS, GIF migrated the application to a cloud environment running various storage clusters, open source cluster management and processing, and web application firewalls.

We're happy to report that we've been extremely successful in conducting these assessments for GIF and they have been very pleased with our work on the effort.

Based on recommendations from GFS and a positive experience with Tevora during the bill pay service sale and migration, GIF selected Tevora to be the QSA to conduct annual PCI DSS assessments for the bill pay services running in the GIF cloud environment. We're happy to report that we've been extremely successful in conducting these assessments for GIF and they have been very pleased with our work on the effort. GIF has now become a significant new client for us.

A Trusted Partner

In our six years working with GFS, we have developed strong working relationships with the GFS team, which makes it rewarding for us and also helps us better understand the unique needs of their business. Based on these deep relationships, our comprehensive knowledge of their environment, and our extensive security expertise, we're often called on to provide strategic advice and conduct security work outside the PCI DSS domain.

ADDITIONAL RESOURCES

Here are some additional Tevora PCI DSS-resources that may be of interest if you'd like to take a deeper dive into this topic.

PCI DSS Compliance Datasheet

Blog Post: Struggling With PCI DSS Compliance? Check Out Our Tips for Addressing 10 Problematic Controls

White Paper: VMware® Validated Design Compliance Kit for PCI DSS

White Paper: Intezer Protect: PCI DSS and HIPAA Security Rule Compliance Review

White Paper: VMware® Software-Defined Data Center (SDDC) Product Applicability Guide for PCI DSS

White Paper: VMware® SDDC PAG for PCI DSS

We Can Help

If you have questions about Tevora's PCI DSS compliance services or would like help bringing your organization into compliance with this important security standard, our team of payment security specialists can help. Just give us a call at (833) 292-1609 or email us at sales@tevora.com.