If you suffer a data breach affecting payment cardholder data, a forensic investigation may be required. Typically, organizations must engage a Payment Card Industry (PCI) Forensic Investigator (PFI) within a certain timeframe after discovering a breach or being notified of an incident by their payment processor or acquiring bank.

Payment card data compromises are tricky business. Looking back to reconstruct the events leading to the breach is a challenge demanding specialized resources capable of dissecting actions and events to determine what happened in the past. VikingCloud is up for the challenge.

VikingCloud has a dedicated forensic investigation practice and performs PFI investigations using proven investigative methodologies and tools. VikingCloud has satisfied all applicable qualification requirements, including PCI Security Standards Council (SSC) required training and qualification proving our knowledge, skill, and experience to perform PFI investigations competently and in line with standards. All VikingCloud PFI Employees are qualified and annually re-certified by the PCI SSC’s program.

Our forensic investigation and analysis help to establish the origin and reason for the compromise, direct corrective actions, and report on our findings and recommendations. And most importantly, we support you through the investigations process and serve as a liaison to payment brands and acquirers, reporting on the issue and what your organization is doing to respond. This ensures all stakeholders are in the know and have the assurance that your organization responded appropriately and is taking action to stop the breach and limit further damage.
**VikingCloud PFI process**

We're the backup plan you hope not to need, but you're thankful you had. You can rely on us when you need a swift response, and you can depend on us for careful scrutinization when it’s most important.

VikingCloud gains a thorough understanding of the situation and explores the distinct aspects of the case by carrying out a series of core activities as part of a defined PFI process.

- Identify the scope of the affected environment
- Conduct discovery and collect evidence
- Perform the forensic analysis
- Produce a preliminary incident response report
- Recommend corrective actions to contain the issue and a risk reduction strategy to limit the impact
- Deliver monthly status and final reporting
- Confirm fixes are operational and effective
- Provide support and, if required, further independent investigation

**Retainer or on-demand rapid response services**

VikingCloud offers two options for engaging with us as your PFI: ad-hoc post-incident or PFI Retainer. A retainer-based relationship provides many advantages, including the following:

- Guarantee we will be available to you
- Quick response—no need to sign contracts in the midst of an incident.
- Facilitate financial planning
- Plan the response strategy ahead of time
- Prioritize clients who have a retainer
- Incentivized service rates

**Why use VikingCloud as your PFI**

VikingCloud is available for a complete investigation to quickly identify the nature of a breach and help you to fill gaps in your security program and safeguard your payment system against future threats. With VikingCloud as your PFI, you always receive the following:

- Qualified expert investigation team and support through the PFI process
- Access to the Asgard PlatformTM for info-sharing and security testing tasks
- Preliminary, periodic and final reporting with recommended corrective actions to safeguard customer data and protect your organization
- Experienced partner for communicating to payment brands and your acquirer

**Why VikingCloud?**

VikingCloud runs some of the largest Level 4 merchant programs in the world, serving over 5+ million merchants. We've spent more than 20 years perfecting our approach to compliance, which blends personalized support with industry-leading technology.