

# ERMProtect PCI PFI Retainer Program

When the card brands require a forensic investigation, organizations have **5 days** to engage a PCI Forensic Investigator. **ERMProtect is one of approximately 20 firms worldwide certified by the PCI Security Standards Council as a PFI.** Our **no-cost retainer** establishes a pre-arranged, contract-ready relationship with our PFI team — so when an investigation is required, a quick and efficient response is guaranteed at pre-negotiated, discounted rates.



## Key Features of Our PCI PFI Retainer Program

- NO-COST RETAINER:** There is no annual fee to maintain the retainer relationship. You secure rapid PFI access and pre-negotiated terms without paying for capacity you may never need.
- PRE-NEGOTIATED TERMS:** MSA, NDA, and rate schedule executed in advance, so there are no contract negotiations while the brands are waiting for an investigation to begin.
- RAPID RESPONSE:** Within 1 business day of intake meeting, the forensic investigation begins – eliminating the 4 to 7 business days typically lost during a crisis.
- DISCOUNTED INVESTIGATION RATES:** If a breach is declared, the first 80 hours of forensic investigation are billed at \$275 an hour. Additional hours are billed at discounted rates.
- VOLUME PROTECTION:** Investigation rates are locked for the duration of the retainer term, even during high-demand periods.
- 15% DISCOUNT ON ADVISORY SERVICES:** Retainer holders receive 15% off tabletop exercises, IR plan reviews, risk assessments, and penetration testing — all measures that lower the risk of a breach.

## Timeframe Guarantees

The retainer is activated by a single phone call or email immediately after notification that a PCI PFI investigation is required. Retainer clients receive guaranteed commitments backed by reserved forensic capacity.

Commitment	Target	Description
Triage call with client	≤ 8 hours	Engagement confirmation, initial scoping conversation, critical preservation directives
Investigation commencement	≤ 1 business day	On-site or remote forensic investigation begins (meets PCI SSC requirement)
Preliminary report	≤ 5 business days	Preliminary report as per PCI SSC requirement is submitted to the card brands and acquirers
Cadence calls	Once a week	ERMProtect-led cadence calls with the brands, acquirers, and the client to update project status and align on open issues
PFI Final Report	Per PCI SSC	Delivered to card brands and client using official PCI SSC report template

## Investment & Pricing Structure

The PCI PFI Retainer is offered with no annual retainer fee. You pay only if an investigation is required, and only for the work performed at pre-negotiated, retainer-discounted rates.

Component	Structure	What It Covers
<b>Annual Retainer Fee</b>	<b>No cost</b>	Pre-signed MSA/NDA, reserved PFI capacity, hotline access, and locked, discounted rates
<b>Discounted PFI Hours (Activated on Breach)</b>	<b>80 hours @ \$275/hr</b>	First block of forensic investigation hours at the retainer-discounted rate
<b>Additional PFI Hours</b>	<b>Time &amp; materials</b>	Hours beyond the discounted block are billed at negotiated, retainer-discounted rates by role (Director, Lead PFI, Consultant)
<b>Advisory Services</b>	<b>15% retainer-program discount on future services</b>	Tabletop exercises, IR plan reviews, risk assessments, and penetration testing
<b>PFI Readiness Engagement</b>	<b>Optional flat fee</b>	Limited, pre-breach engagement to position your team and ours for a rapid response

## Optional Readiness Engagement

In a limited scope engagement of <2 days, we get to know your environment, infrastructure, incident response plan, and logging practices before – not during – a crisis. Embedded with your team, we spot and remediate issues that commonly trip up PCI PFI investigations. This pre-crisis engagement lowers risk, eliminates hours spent on the learning curve, and positions your team and ours to move forward on Day 1 – not Day 3.

### SIX FOCUS AREAS

 <b>CDE Scope &amp; Dataflow</b>	 <b>Network Topology</b>	 <b>IR Plan &amp; Evidence-Handling Playbooks</b>
 <b>Detection &amp; Monitoring Capability</b>	 <b>Logging Coverage</b>	 <b>Report on Compliance (ROC)</b>

**Independence Preserved.** Because PCI rules require the PFI to remain independent of the entity it investigates, the Readiness Engagement is structured as consulting work and not as QSA audit work, monitoring, or managed security services. This preserves ERMProtect's ability to serve as your PFI.

## Why ERMProtect



### PCI PFI Certified

One of approximately 20 firms worldwide authorized by the PCI Security Standards Council to investigate card breaches.



### Full PCI Credential Stack

PFI + QSA + ASV under one roof, giving end-to-end visibility into payment environments.



### 27+ Years in Cybersecurity

Experience handling breaches with hundreds of servers and millions of compromised records for prominent brands in multiple industry verticals.



### Geographic Coverage

Clients across the US, Canada, Latin America, the Caribbean, and Europe; bilingual English/Spanish delivery.