

# Fable Security & PCI DSS Compliance

How Fable helps you meet, and prove, the human-risk requirements of PCI DSS 4.0, for any organization that touches cardholder data: retail, hospitality, and financial services alike.

## The problem: PCI DSS made the human layer a real control

PCI DSS 4.0 turned Requirement 12.6 from a once-a-year module into an operating control with teeth: a documented program, reviewed at least every 12 months, role-based content covering phishing and social engineering, and, under the 4.0.1 update effective March 31, 2025, explicit coverage of acceptable use of end-user technologies. QSAs now ask for more than a completion report: role-based content mapped to policy, personnel who can explain their responsibilities, and documented exception handling.

Most legacy awareness tools were built for the box that used to exist: an annual video, a quarterly click rate, a spreadsheet of completions. That doesn't satisfy this bar, and it gives your board and acquiring bank no real evidence that a cashier, call center agent, or AP clerk is actually less likely to hand over cardholder data under pressure.

The MGM Resorts breach is what that gap looks like in a payments environment: a \$100M+ loss that started with a single help-desk social-engineering call. Identity verification and MFA-reset workflows are exactly the moments a completion report can't speak to.

## Requirement-by-requirement: where Fable fits

| PCI DSS 12.6                                                                   | WHAT IT REQUIRES                                                                                                                                                                               | HOW FABLE DELIVERS                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>12.6.1 / 12.6.2</b><br>Formal, documented awareness program                 | A formal security awareness program must be documented, and reviewed and updated at least once every 12 months and whenever new threats or vulnerabilities emerge. (Effective March 31, 2025.) | Fable is a program, not a campaign calendar: Detect → Evaluate → Act → Prove runs continuously and documents itself. Interventions update the moment new threat signals appear (Genesys got a custom phishing video in about a day), so “reviewed and updated” is the default state, not an annual scramble.                                   |
| <b>12.6.3</b><br>Training upon hire and at least annually, with acknowledgment | All personnel receive security awareness training at hire and at least once every 12 months, with records showing who completed it and when.                                                   | Role- and cohort-based enablement (cashiers, call center agents, AP/finance, engineers with cardholder data access), kept current against modern social engineering like vishing, deepfakes, and AI-driven scams instead of a static annual video, with per-person, per-date attestation records built for QSA review, not just an LMS export. |

### 12.6.3.1

Phishing and social-engineering awareness

Training content must address phishing and related social-engineering attacks relevant to the organization's actual environment.

Multi-channel simulation and coaching (phishing, vishing, MFA-fatigue, deepfake impersonation) targeted at the roles attackers actually go after in payment environments: help desk identity verification, AP payment approval, and frontline staff with cardholder access.

### 12.6.3.2

Acceptable use of end-user technologies

Training must cover acceptable use of end-user technologies, including the tools employees adopt on their own.

Policy Boost turns your existing Acceptable Use Policy into role-specific briefings with tracked, dated attestation. Shadow AI detection flags employees pasting cardholder or sensitive data into unsanctioned AI tools, the newest version of this requirement QSAs are starting to probe.

### 12.6 (program-wide)

Evidence beyond completion records

QSAs increasingly ask for more than a completion report: role-based content mapped to policy, personnel who can explain their responsibilities, and documented exception handling for anyone who missed training.

The Prove step measures behavior change per person and per cohort, tied to the specific intervention that caused it. Sisense calls it out by name as “a full audit trail.” Non-completers escalate automatically instead of falling through a spreadsheet.

## Proof, not promises

#### SISENSE

**Audit-grade evidence.** Sisense names Fable's “full audit trail” as the reason GRC and compliance teams can defend the program to auditors, not just report on it.

#### PENNYMAC

**Behavior change that holds up in a regulated environment.** Pennymac (regulated financial services) saw a 2.4x higher phishing reporting rate when employees received a Fable briefing versus when they didn't, and CISO Cyrus Tibbs points to a measurable link between engagement and reduced vulnerability.

## Why now

The 4.0.1 changes are already in force, and regulators, boards, and QSAs are done accepting completion percentages as proof of anything. Organizations that move to a measured, evidenced, closed-loop program won't just pass their next assessment. They'll walk in with a story about reduced human risk that the assessor, the board, and the acquiring bank can all trust.

This document maps Fable's capabilities to PCI DSS 4.0.1 Requirement 12.6 for informational purposes. Confirm control mapping for your specific assessment with your QSA.