MALA TECHNOLOGY ADVISORS

Independent Technology Guidance. Market Intelligence. Better Decisions.

RETAIL · INDUSTRY DATA SHEET

# Technology Risk Advisory for Retail Organizations.

Retailers run on thin margins, seasonal peaks and a sprawl of POS, e-commerce, payment and store-network vendors. Ransomware, PCI DSS 4.0 and third-party risk now reach every checkout. MALA benchmarks your store, e-commerce and payment technology, then sequences fixes around your selling calendar. Start with a no-fee initial assessment.

PCI DSS 4.0 + Store Networks + POS & E-commerce + Ransomware Resilience + **No-Fee Initial Assessment**

THE CHALLENGE

## Every store, site and vendor is part of the attack surface.

### Payment page exposure
PCI DSS 4.0 now requires monitoring every script on the checkout page.

### Store network sprawl
Hundreds of locations, each with POS, Wi-Fi and IoT to secure.

### Vendor overload
POS, e-commerce, loyalty and logistics vendors, each with access.

### Downtime at peak
An outage in Q4 costs sales you can't recover in Q1.

OUR APPROACH

## Fixes scheduled around your selling calendar.

**01 Map**
Inventory stores, POS, e-commerce and payment flows.

**02 Scope**
Confirm PCI DSS 4.0 scope, including payment-page scripts.

**03 Benchmark**
Compare network, POS and SaaS contracts to market pricing.

**04 Test Resilience**
Review backups, segmentation and store failover.

**05 Sequence**
Schedule remediation outside peak and freeze windows.

*PCI DSS 4.0 requirements 6.4.3 and 11.6.1 for payment-page scripts became mandatory on March 31, 2025.*

HOW MALA HELPS

## A Retail Technology Reality Assessment.

### PCI DSS 4.0 gap map
Current state against the requirements now in force.

### Store network review
SD-WAN, Wi-Fi and failover evaluated across locations.

### POS & e-commerce review
Platforms, integrations and payment flows in one view.

### Vendor risk program
Every provider with store or customer data access, verified.

### Ransomware resilience
Backup integrity, segmentation and response readiness.

### Cost & contract benchmark
Network, POS and cloud spend against market pricing.

*Most retail environments carry more vendors with network access than anyone has listed. The assessment starts there.*

BY THE NUMBERS

## Why this matters now.

**$1.65M**
average ransomware recovery cost for retailers, excluding ransom
SOPHOS STATE OF RANSOMWARE IN RETAIL 2025

**58%**
of retailers whose data was encrypted paid the ransom
SOPHOS STATE OF RANSOMWARE IN RETAIL 2025

**Mar 2025**
PCI DSS 4.0 payment-page script requirements became mandatory
PCI SECURITY STANDARDS COUNCIL

**$0**
for your initial assessment. No obligation to move forward
NO-FEE INITIAL ASSESSMENT

WHO IT'S FOR

## Built for the people who own the decision.

| | |
|---|---|
| **Multi-location Retailers** | Consistent security and connectivity across every store. |
| **E-commerce & Omnichannel** | Checkout and payment pages that hold up to PCI DSS 4.0. |
| **CIO / CISO** | Store, cloud and vendor gaps ranked by exposure. |
| **CFO / Finance** | Technology spend benchmarked against market pricing. |
| **Store Operations** | POS and store systems that stay up through peak season. |

THE MALA MODEL

## Unbiased. Vendor-sponsored.

Our services are sponsored through strategic referral agreements with 330+ technology solutions providers, never billed to you. MALA is paid by the vendor only if you move forward with a vendor we recommend.

- **Unbiased recommendations**
  Providers within each category have similar compensation models, so your requirements drive the answer.
- **Paid only if you move forward**
  The selected vendor compensates MALA, and only when you choose a recommended vendor.
- **No obligation**
  You are never required to move forward with any recommended vendor.

COMMON QUESTIONS

## What clients ask first.

**Q What changed in PCI DSS 4.0?**
Payment-page scripts must be inventoried, authorized and monitored for tampering, and the future-dated requirements are now enforced.

**Q Why is ransomware different in retail?**
Downtime stops sales at every register and site at once, and peak-season losses can't be made up later.

**Q What does it mean for our vendors?**
Every provider that touches store networks or cardholder data needs defined responsibilities and ongoing verification.

**Q Can this wait until after the holidays?**
The assessment can start anytime. Remediation is sequenced around your freeze windows.

ENGAGEMENT AT A GLANCE

| | |
|---|---|
| **Scope** | Stores, e-commerce, payments and the vendors behind them |
| **Focus** | PCI DSS 4.0, store networks, vendor risk and ransomware resilience |
| **Deliverable** | Roadmap sequenced around your selling calendar |
| **Cost to you** | No-fee initial assessment. Vendor-sponsored, no obligation |

SERVICES: Reality Assessment · Cybersecurity · Network & Connectivity

NO-FEE INITIAL ASSESSMENT

## Request your no-fee Retail Technology Risk Assessment. No obligation.

We review your stores, e-commerce and payment environment against PCI DSS 4.0, covering store networks, vendor access and ransomware resilience.

Vendor-sponsored: MALA is paid by the vendor only if you move forward with a recommended vendor. No obligation to do so.

## Let's simplify your next technology decision. Talk to an advisor.

**Eric Anderson**
eanderson@malatechadvisors.com
+1 (603) 802-2469 · malatechadvisors.com