PCI Compliance - What You Need To Know and Common Challenges

FSFOA November 2026 Conference

November 4, 2026

© RSM US LLP. All Rights Reserved.

Presenter

Greg Moody
Manager
Greg.Moody@rsmus.com
574 283 2715
South Bend, IN



Certifications:

- Qualified Security Assessor
- Certified Information Systems Security Professional
- Certified Information Systems Auditor

© RSM US LLP. All Rights Reserved.

Agenda

Topic	Minutes
Welcome and outcomes	3
PCI basics, school payments, and scope	16
Vendor oversight and payment approvals	3
Common operational challenges	13
School scenario, governance, and action plan	10
Questions and answers	5
Total session	50

© RSM US LLP. All Rights Reserved.

Why payment security belongs on the finance agenda

A familiar school-district scenario

Families pay online, at school offices, at athletic events and through third parties. Yet no single process owner may have a complete view of the channels, vendors, devices or evidence.

The question is not “Who completes the SAQ?”

It is “Can we demonstrate that every payment channel is known, governed and secure?”

1

Protect families

payment information

2

Avoid disruption

to collections and services

3

Preserve trust

with leadership and communities

4

Define ownership

across finance, IT and schools

RSM

© RSM US LLP. All Rights Reserved.

School payments: more than the business office

- Online: meal accounts, activity fees, aftercare, and event registration.
- In person: ticket offices, bookstores, concessions, and school offices.
- Staff-assisted: telephone payments and approved virtual terminals.
- Inventory each channel, merchant account, vendor, device, and school owner.
- Include booster groups and outside operators when they use school accounts or systems.

© RSM US LLP. All Rights Reserved.

PCI in plain English: four ideas to remember

1. **Know the payment paths**
   Inventory online, in-person and staff-assisted channels, including merchant accounts, vendors and devices.

2. **Minimize card-data handling**
   Use approved hosted services and avoid card data in email, spreadsheets, chat or recordings.

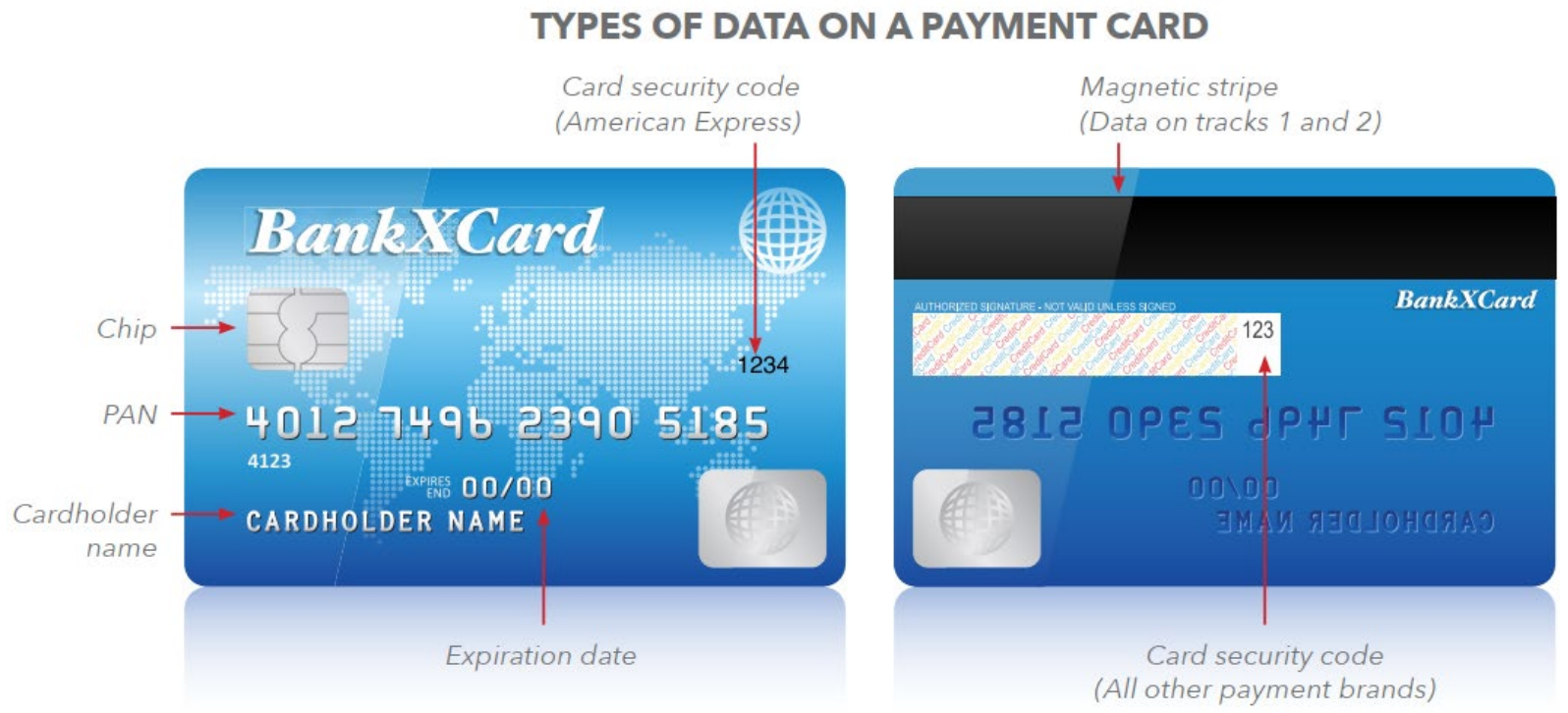
3. **Outsourcing does not outsource accountability**
   Confirm what the provider covers, what the district retains and what evidence must be maintained.

4. **Evidence matters all year**
   A signed SAQ is supported by inventories, access reviews, vendor records, testing and issue resolution.

© RSM US LLP. All Rights Reserved.

PCI DSS primer—Account data

- The PCI DSS applies to **ANY** organization that stores, processes or transmits credit or debit card account data or can impact the security of account data.



Source: https://www.pcisecuritystandards.org/pci_security/why_security_matters

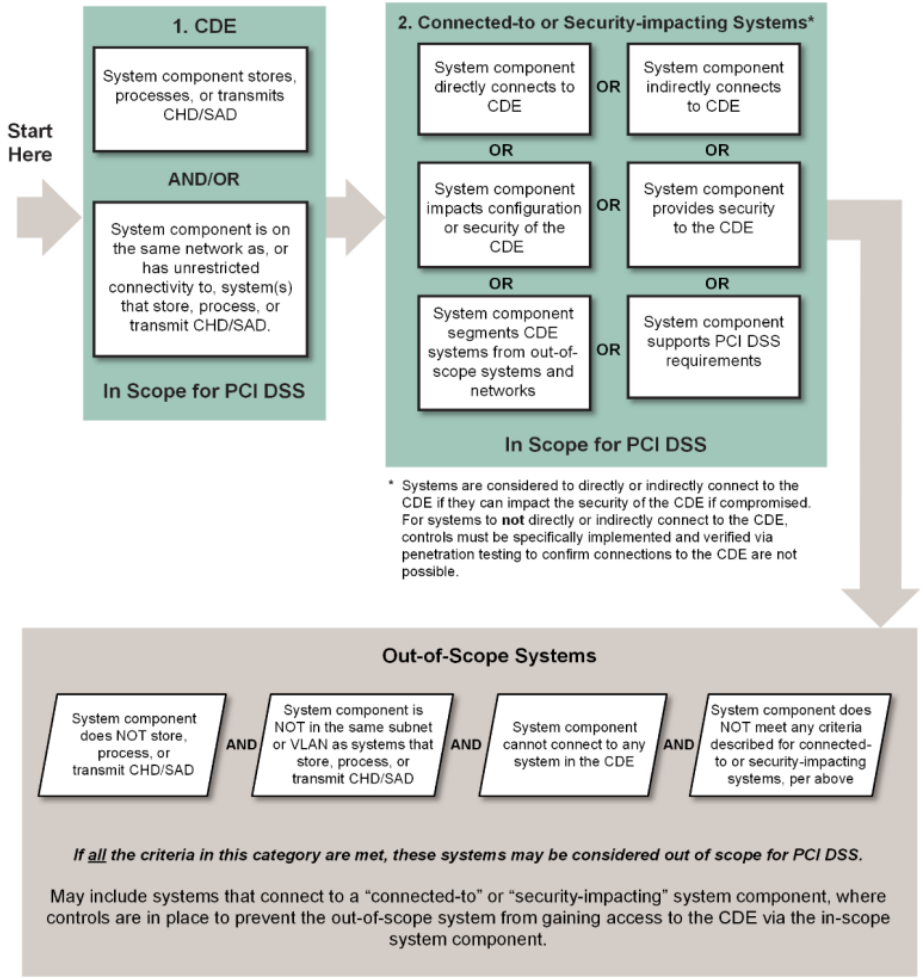
© RSM US LLP. All Rights Reserved.

PCI DSS primer—Key terms

- **Primary account number (PAN)**—The credit or debit card number
- **Cardholder data (CHD)**—Payment card information (e.g., PAN, expiration date)
- **Sensitive authentication data (SAD)**—CVC/CVV, track data from magnetic strip or EMV chip
- **Merchant**—Entity that accepts payments cards for payment
- **Service provider**—Business entity that is not a payment brand and directly involved in the processing, storage or transmission of cardholder data on behalf of another entity
- **Self-Assessment Questionnaire (SAQ)**—Reporting for Level 2, 3 or 4 merchant assessments

© RSM US LLP. All Rights Reserved.

PCI DSS primer—Cardholder data environment scope



- The standard applies to:
  - People, processes and technologies (system components) **that store, process and transmit CHD or SAD**
  - System components that may **not** store, process or transmit CHD/SAD but have **unrestricted connectivity** to system components that store process or transmit CHD/SAD
  - People, processes and system components that could **impact the security of the CDE**

Source: https://www.pcisecuritystandards.org

© RSM US LLP. All Rights Reserved.

Card data handling and scope

- Limit primary account number (PAN) collection and retention to documented business needs.
- Do not retain card verification codes such as CVV after authorization, even if encrypted.
- Masking hides digits on screen. It does not remove the underlying full card number.
- Encryption and tokenization may reduce exposure. Scope depends on the implementation.
- Avoid collecting card data in email, spreadsheets, chat, or call recordings.

© RSM US LLP. All Rights Reserved.

Reducing payment scope

Use approved hosted payment services where families enter card data directly.

- For terminals, evaluate PCI-listed point-to-point encryption (P2PE) solutions.
- Separate payment environments from unrelated networks where appropriate.

Document the actual data flow, including refunds, reports, and support access.

Reassess scope when a school adds a payment channel, device, or vendor.

© RSM US LLP. All Rights Reserved.

Vendor oversight: questions before approval

- Does the current Attestation of Compliance cover the exact service we use?
- Which controls does the vendor perform, and which remain with the school?
- What implementation steps and ongoing evidence must the school maintain?
- Who reports incidents, service changes, and changes in compliance status?
- Who reviews vendor evidence and the responsibility agreement each year?

© RSM US LLP. All Rights Reserved.

What happens when payment compliance breaks down?

Financial

Processor or bank fees
Forensic and remediation cost
Legal, notification and advisory expense

Operational

Payment interruption
Emergency staff effort
Delayed registration, meals, fees or events

Governance

Unknown owners or systems
Missing evidence
Audit and leadership escalation

Trust

Family and community concern
Public scrutiny
Reduced confidence in district stewardship

PCI noncompliance is not just a failed questionnaire. It can become a financial, operational and leadership event.

RSM

© RSM US LLP. All Rights Reserved.

School scenario: a busy registration evening

- Illustrative scenario: the fee portal is unavailable during registration.
- A staff member proposes recording card numbers in a spreadsheet for later entry.
- Discussion: what should staff do, and whom should they contact?
- Safer response: use an approved alternative or defer payment. Avoid creating an unapproved card-data store.
- Follow-up: document the issue and improve the outage procedure.

© RSM US LLP. All Rights Reserved.

Common challenge: fragmented ownership

- Gap: individual schools buy payment tools without central review.
- Finance owns the merchant inventory, bank coordination, and validation calendar.
- IT owns technical scope, access controls, and security evidence.
- School staff own approved procedures, device checks, and prompt reporting.
- Leadership assigns one accountable coordinator and a process for approving changes.

© RSM US LLP. All Rights Reserved.

Common challenge: shared and outdated access

- Give each user an individual account with access limited to job duties.
- Apply required multi-factor authentication for access into the cardholder data environment.
- Remove access promptly when staff leave or change roles.
- Control vendor access and review accounts, including seasonal staff.
- Evidence: approved access, reviews, offboarding records, and authentication settings.

© RSM US LLP. All Rights Reserved.

Common challenge: payment devices and paper

- Keep a current inventory of terminals, serial numbers, and assigned locations.
- Inspect devices for tampering or substitution at the defined frequency.
- Train staff to verify repair personnel and report unfamiliar devices.
- Secure paper records containing account data and destroy them when no longer needed.
- Plan how schools control terminals during events, transport, and storage.

© RSM US LLP. All Rights Reserved.

Common challenge: maintenance between assessments

- Keep payment software and supporting systems on supported versions.
- Assign owners and deadlines for security patches and vulnerability remediation.
- Perform required scans and testing, then retain evidence of fixes and retesting.
- Include school-hosted webpages that redirect to or embed payment services in the review.
- Escalate overdue items before the annual assessment.

© RSM US LLP. All Rights Reserved.

Common challenge: missing compliance evidence

- Keep the payment inventory and data-flow documentation current.
- Retain evidence of access reviews, security monitoring, and issue resolution.
- Use targeted risk analyses where requirements allow a risk-based frequency.
- Maintain vendor evidence, training records, and an incident-response exercise record.
- Treat the SAQ and AOC as supported attestations, not a box-checking exercise.

© RSM US LLP. All Rights Reserved.

Common challenge: staff workarounds

- Give school staff a short, approved payment-handling procedure.
- Train staff to recognize phishing and suspicious terminal changes.
- Direct families to the approved payment method instead of requesting card details by email.
- Provide a safe procedure for refunds and payment-service outages.
- Include temporary and seasonal personnel, and reinforce training when processes change.

© RSM US LLP. All Rights Reserved.

Suspected incident: immediate escalation

- Report suspected payment-data exposure through the school's incident-response process immediately.
- Engage the designated response team, payment provider, and acquiring bank as the plan requires.
- Preserve evidence and coordinate containment with qualified responders.
- Follow established procedures for card data found in an unexpected location.
- Test and review the incident-response plan at least annually.

© RSM US LLP. All Rights Reserved.

A 90-day plan for school leadership

- Days 1–30: inventory payment channels and merchant accounts. Name the finance and IT owners.
- Days 31–60: confirm scope and SAQ eligibility with the bank. Review vendor evidence and responsibilities.
- Days 61–90: close priority gaps, rehearse incident response, and assemble assessment evidence.
- Track progress with a named owner, due date, and completion evidence for each action.

© RSM US LLP. All Rights Reserved.

PCI is one part of broader cyber resilience

Identity & access

Unique accounts, least privilege, MFA and timely offboarding

Third-party risk

Provider due diligence, contracts, responsibilities and ongoing monitoring



Vulnerability management

Supported systems, patching, scanning and remediation evidence

Incident response

Escalation, evidence preservation, exercises and coordinated recovery

Position adjacent services as answers to the risks already discussed, not as a separate service catalog.

© RSM US LLP. All Rights Reserved.

Key takeaways for school leaders

- Know where and how your schools accept card payments.
- Reduce unnecessary handling of card data and approve new payment services centrally.
- Confirm scope and SAQ eligibility using the actual environment.
- Keep named owners and evidence throughout the year.
- Ask: what payment risk will our finance and IT teams address first?

© RSM US LLP. All Rights Reserved.

QUESTIONS AND ANSWERS

© RSM US LLP. All Rights Reserved.

THANK YOU FOR YOUR TIME AND ATTENTION

© RSM US LLP. All Rights Reserved.

Appendix

© RSM US LLP. All Rights Reserved.

Florida HB 967: more online payments, more governance

JAN 1 2027

Effective date

Chapter 2026-169

Required for covered units of local government

What the law says

Covered units must accept specified electronic payment methods for obligations owed to them, except where another form is required by law, and must provide an online payment method.

Why finance should care

Any expansion of online channels can add vendors, integrations, merchant accounts, refund paths, reconciliation processes and cybersecurity dependencies.

Important audience caveat

The official summary expressly lists municipalities, counties, special districts and county constitutional officers. It does not expressly list school districts.

Recommended message

Confirm applicability with district counsel. Regardless, use HB 967 as a timely prompt to inventory payment obligations, channels and security ownership before adding online options.

RSM

© RSM US LLP. All Rights Reserved.

If online payments expand, govern the change before go-live

1

Obligations

List every fee, charge and receivable collected across the district.

2

Channels

Identify which are online, in person, telephone-assisted or handled by a third party.

3

Design

Prefer architectures that minimize district handling of card data.

4

Due diligence

Review provider AOC, service scope, responsibilities, integrations and incident terms.

5

Operations

Define refunds, exceptions, reconciliation, outages, access, monitoring and evidence.

Control objective: convenience should increase without creating unknown payment paths or unowned risk.

RSM

© RSM US LLP. All Rights Reserved.

SAQs for online and outsourced payments

- SAQ A: fully outsourced card-not-present payments, with no electronic account data on school systems or premises.
- SAQ A-EP: e-commerce where the school website can affect payment security without receiving card data.
- SAQ D for merchants: the route when the environment does not meet another SAQ's eligibility criteria.
- A vendor's product label does not decide eligibility. Confirm every criterion and your bank's instructions.

© RSM US LLP. All Rights Reserved.

SAQs for terminals and staff-assisted payments

SAQ P2PE: eligible use of a PCI-listed validated P2PE solution.

- SAQ SPI: eligible standalone, approved-PTS-connected payment terminals.
- SAQ C-VT: eligible isolated computers used for manual virtual-terminal entry.
- SAQ B or C: specific dial-out terminal or payment-application environments.
- These are starting points, not eligibility determinations. Review all school payment channels with your bank.

© RSM US LLP. All Rights Reserved.