2025 NORTH AMERICA COMMUNITY MEETING

Beyond the Vendor

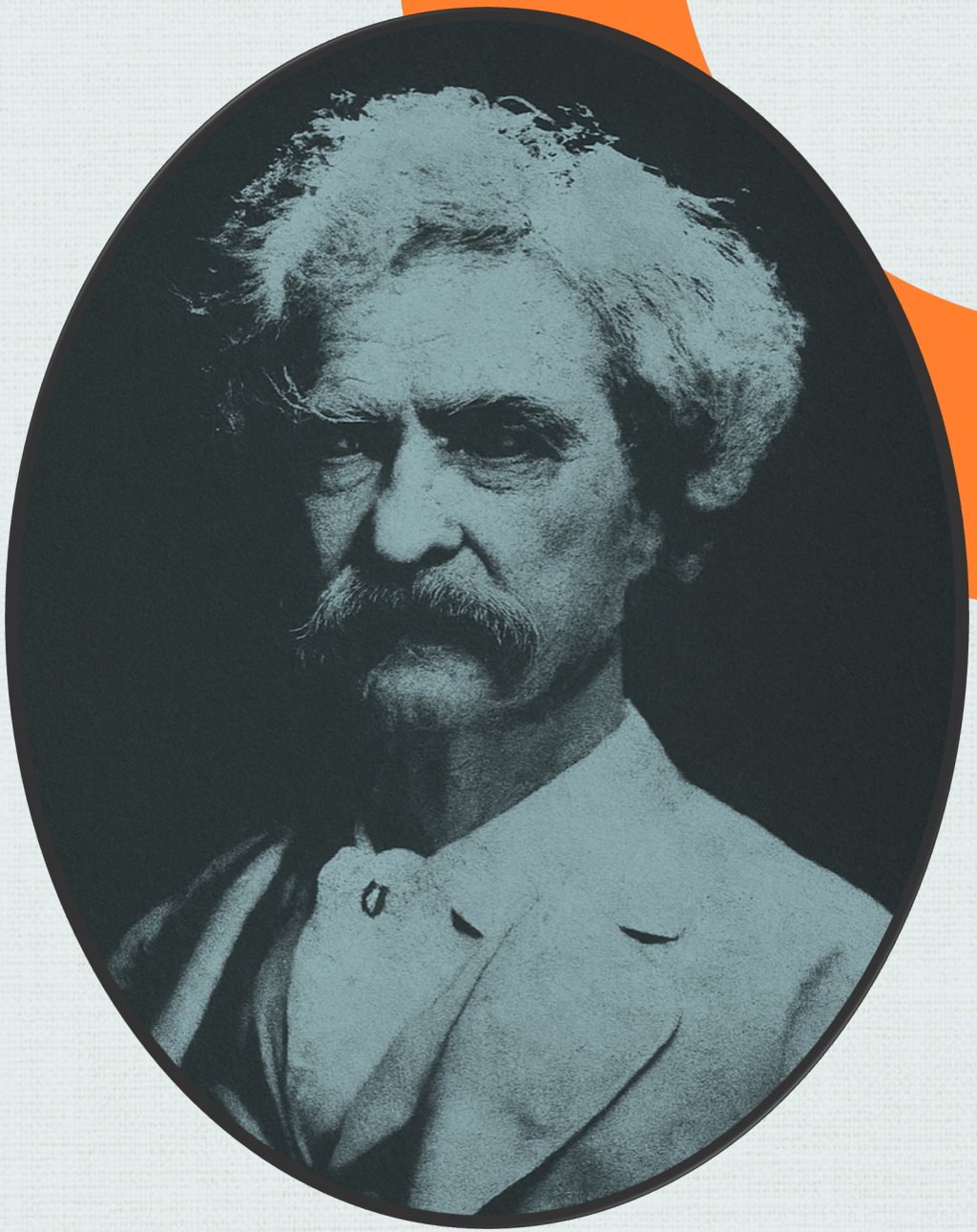
Managing Fourth, Fifth, and Nth-Party Risks in PCI Environments

It's not the things you don't know that get you into trouble.

~

It's the things you know for sure that just ain't so.

- Mark Twain



Brian Willis

QSA, CISSP, ISO 27001 LA
Partner
LBMC

Kyle Hinterberg

QSA, CISSP, CISA, AWS SCS
Sr. Manager
LBMC

Compliant Third Parties

≠

Secure Ecosystem

Real-World Example

The biggest data theft of 2023

Popular file transfer solution

- A ransomware group exploited an unauthenticated SQL injection vulnerability
- The ransomware group leveraged this vulnerability to gain remote code execution
- The ransomware group proceeded to exfiltrate data from the file transfer solution's environment
- Over 2,000 organizations and 95,000,000 individuals are believed to have been affected
- Many of these organizations were unaware that their data was being stored or transmitted by this solution!

Real-World Example

The biggest data theft of 2023

- Multiple major UK organizations
  - All used a third-party payroll solution
  - The payroll provider used the file transfer solution
  - ~34,000 staff had their data compromised
- 900+ U.S. higher education institutions
  - All relied on a national student data service
  - The student data service used the file transfer solution
  - ~270,000 students had their data compromised
- A large U.S. retirement and insurance association
  - Used a third-party research service
  - The research service used the file transfer solution
  - Over 371,000 retirement plan participant records were compromised

PCI DSS Requirements & Guidance

Requirement 12.8 – Risk to information assets associated with third-party service provider (TPSP) relationships is managed.

Requirement 6.4.3 Applicability Notes – This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties.

PCI FAQ 1588 – A provider of third-party scripts is not considered a third-party service provider (TPSP) for purposes of SAQ A, if the provider's only service is providing scripts not related to payment processing and where those scripts cannot impact the security of cardholder data and/or sensitive authentication data.

Information Supplement: Third-Party Security Assurance – When a TPSP outsources services (nested TPSPs), it can affect PCI DSS scope and risks. Entities should ensure they are notified of such outsourcing, define clear contractual limits and responsibilities, and consider oversight of these nested providers, even though formal monitoring is only required for directly contracted TPSPs.

12.8.1: A List of all TPSPs is Maintained

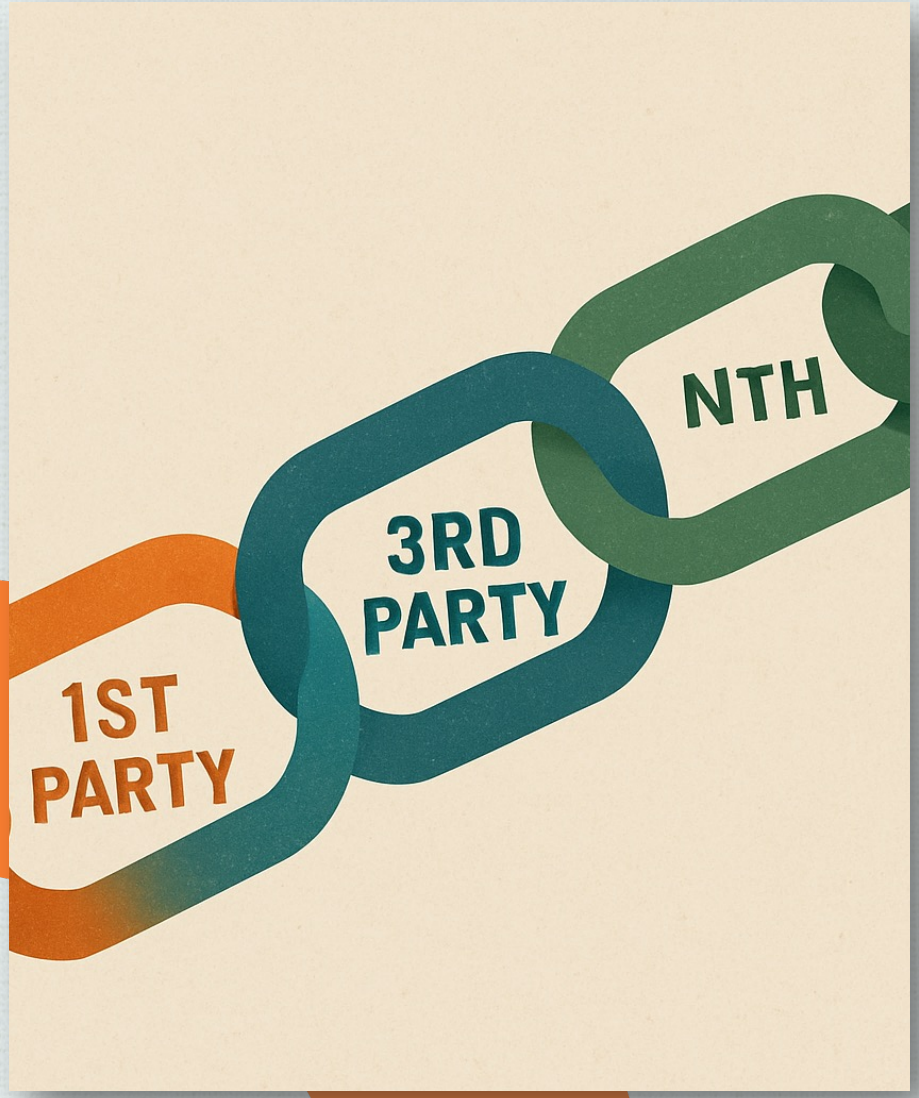
Do you know who your service providers and their service providers are?

- Keep a vendor registry
- Include all vendors who S/P/T CHD, manage CDE system components, or are security impacting (MSS, SW Dev)
- Research & document vendors listed in their attestations
- Review Nth party attestations and monitor them; check vendor and Visa websites and document these to support 12.8.4
- 12.8.5 says it is the responsibility of the primary TPSP to manage/monitor their providers, but entities can do this too

12.8.2: Written Agreements Maintained

Are your TPSPs acknowledging their security and compliance responsibilities to the Nth degree?

- Review service agreements prior to signing on
- Involve internal or external legal counsel
- Are nested service providers addressed in agreements?
- DSS only requires acknowledgement they are “responsible for the security of account data…”
- TPSPs *must* provide per 12.9.1; consider making this a condition of service



12.8.3: Due Diligence

Have you properly vetted *all* parties?

- Security/compliance should be plugged into your vendor vetting, management, review program
- Review *all* vendors to identify those that could affect security of account data even if not directly payment related
- Consider ability to monitor related requirements (e.g., 6.3.1)
- Review vendor website(s), attestations, press releases, etc.
- Consider vendor monitoring services for security incidents, reputation
- Ask your network

12.8.4: TPSP Compliance Monitoring

Are they holding up their end of the bargain?

- Review annually = at least once every 365 days
- Solicit attestations and be wary of significant delays
- Review Visa Global Registry website for primary and nested vendors
- Review attestations against agreements
- Validate the attestation covers your service(s)
- Have your QSA review

12.8.5: TPSP Compliance Responsibilities

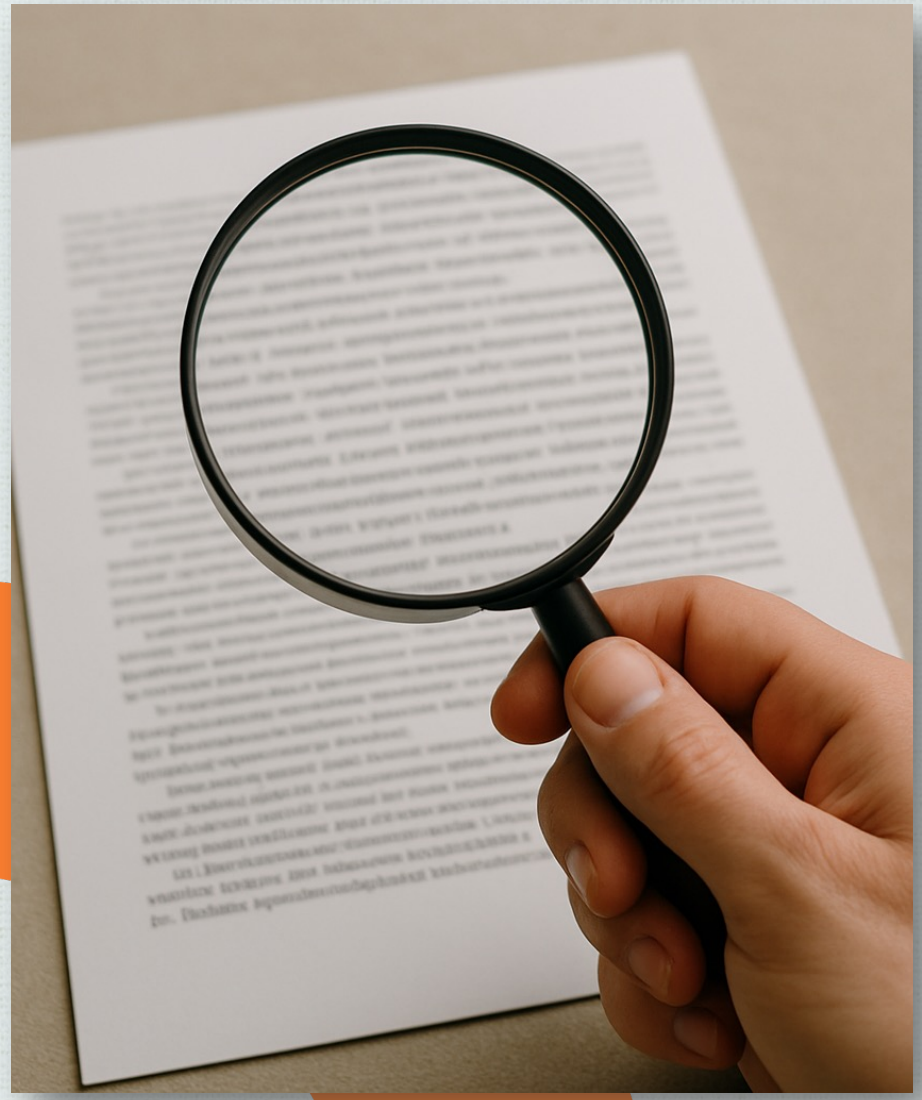
Which requirements are yours, mine, and ours?

- TPSPs must provide per 12.9.2
- DSS only requires that “information is maintained…” but entity should document this independently of vendor-provided records
- Good Practices:
  - Responsibility Matrix
  - DSS mentions importance of monitoring *nested TPSPs*
  - “Note that it is the responsibility of the primary TPSP to manage and monitor any secondary TPSPs.”

LBMC

Third-Party Service Provider Responsibility Matrix

PCI DSS Requirements v4.0.1	Responsibility	4th-party dependencies	Specific coverage/scope of responsibilities	How and when TPSP will provid evidence of compliance to entity	Notes
Requirement 1: Install and Maintain Network Security Controls					
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.					
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.					
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	Entity Third-Party Service Provi Shared				
1.2 Network security controls (NSCs) are configured and maintained.					



Non-Attested Third-Party Service Providers

Well, somebody has to do it.

- Must be monitored for compliance per 12.8.4
- Good Practices:
  - TPSPs “may be able to provide other sufficient evidence to demonstrate that it has met the applicable requirements without undergoing a formal compliance validation.”
  - “…can provide specific evidence to the entity’s assessor…”
  - “…can elect to undergo multiple on-demand assessments…”
- This should be worked out as part of agreements to cover costs and risk of assessing
- Not easy to request after the fact

Don’t go it alone – Engage experts

Payment Card Industry
Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

Continuous Monitoring

- Use of third-party risk monitoring platforms
- Threat intelligence specific to supply chain risks
- Real-time visibility into key vendor relationships

6.3.1 Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

Are we Really Managing the Risk?

- ❑ Do we maintain a complete, current inventory of all TPSPs?
- ❑ Do we know who our vendors rely on (4th, 5th, Nth parties)?
- ❑ Are subcontractors explicitly addressed in our contracts?
- ❑ Have we reviewed and validated attestations, not just collected them?
- ❑ Have we defined who owns what in a responsibility matrix?
- ❑ Are we monitoring TPSPs at least annually and when risks change?

Compliant Vendor Management

≠

Resilient Ecosystem

Thank You

Brian Willis
brian.willis@lbmc.com
linkedin.com/in/brianswillis

Kyle Hinterberg
kyle.hinterberg@lbmc.com
linkedin.com/in/kylehinterberg

Visit us at
Booth #27 in the
Vendor Showcase

LBMC

www.LBMC.com

PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING