Approaches for Monitoring Third Party Service Providers (TPSPs) Workshop Notes and Outcomes

North America Community Meeting

PCI Security Standards Council®

Approaches for Monitoring Third Party Service Providers (TPSPs) Workshop

Facilitator

Toast, Inc. – Shane Hamilton

Recorder(s)

Patrick Shuman, Lynne Feldstein, Cathleen Levie, Samantha Silva

Goals:

- **Share Program Structures:** Encourage participants to describe the structure and key elements of their TPSP monitoring programs. Highlight variations in program design and execution across different organizations.
- **Detail Review Processes**: Discuss how participants conduct reviews of third-party service providers. Explore different methods, tools, and criteria used during these reviews.
- **Exchange Information Requests:** Share what specific information and documentation participants ask for from their third-party service providers. Identify commonalities and differences in information requirements.
- **Discuss Response Strategies:** Examine how participants respond to the information gathered from their third-party service providers. Discuss strategies for addressing non-compliance or inadequate responses.
- **Generate Innovative Solutions:** Brainstorm innovative solutions to improve the monitoring of third-party service providers. Encourage participants to think creatively and consider new approaches.
- **Create Actionable Takeaways:** Ensure participants leave the workshop with clear, actionable insights and steps they can implement in their organizations. Summarize key points, best practices, and agreed-upon action steps for future reference.

Objective:

To share and discuss ideas, experiences, success stories, and lessons learned related to monitoring TPSPs. Participants will identify best practices, common challenges, and strategies for driving industry-wide improvement.

This workshop aims to enhance participants' understanding and execution of TPSP monitoring programs, foster the development of innovative solutions, and create a collaborative environment for ongoing improvement.

Identify Best Practices:

- Each group to discuss best practices and challenges in monitoring TPSPs.

Identify Challenges & Strategies:

- What success stories can you share regarding TPSP monitoring?
- What lessons have you learned from challenges faced in monitoring TPSPs?
- How have these experiences shaped your current monitoring approach?

Identify Actions:

- **Organizations:** Identify action step they will take back to their organization.
- **PCI SSC:** Identify actions for PCI SSC (develop guidance, training module, addition to standard or qualification requirements)

Approaches for Monitoring Third Party Service Providers (TPSPs) Workshop – Boston Outputs

Moderator: Toast, Inc. – Shane Hamilton

Identify Best Practices:

- Roles and Responsibilities
- Auditing TPSPs
- Strong Contracts
- Insight into TPSPs
- Inventory of TPSPs
- Risk-based approaches
- Education
- Communication
- Avoid a one-size-fits-all
- Due diligence
- Ensure Proper Staffing

Identify Challenges:

- Communications
  - Clear line of communication with TPSPs
    - regular meetings – especially when changes occur at the TPSP
  - Lack of mature process liaisons
- Precheck/proactive approach
- Education of TPSPs
- Building strong relationships

Identify Strategies:

- Trust but Verify
- Define what services TPSPs provide
- Documented Scope
- Get involved early
- Communication
- Monitoring Process
- Categorize TPSPs
  - create a risk-based schedule for monitoring/audit – even if not necessarily involved in payments
- Challenge pushback from TPSPs

Identify Challenges & Strategies:

- Sending Alerts and Reminders
- Relationship with Legal
- Appropriate staffing and Education of staff
- Meetings
  - Increased frequency of touchpoints
- Accountability
- Evolve Programs as needed

Proposed Actions (Organizations):

- Level setting
- Update Legal Language
- Increasing Communication
- Education
- Glossary of PCI terms for organization

Proposed Actions (PCI SSC):

- Guidance/Communication
  - TSP delegation, similar to guidance on Scoping and Segmentation and Pen Testing – Simple and not too prescriptive
  - Updated FAQs
  - Infographics
  - Case Studies/Examples
- Guidance/Communication
  - Brand AOC requirements
  - Roles and Responsibility Matrix Template (Excel/Spreadsheet format)
  - Clarification of acceptable Compliance Documents
  - Example contract language
- TPSP Listing Program
  - for certified vendors who have PCI validated services to see list of PCI compliant vendors
- Training
  - Maintaining relationships with TPSPs
- AOC Update
  - summary with signature (as pre-pendix)
- Workshops
  - More workshops like these
- Standards
  - How short-term risk decisions by TPSP are to be managed day-to-day

Next Steps:

- EUCM Workshop outputs to be incorporated after October meeting
- PCI SSC and Executive Committee to review in November
- Board of Advisors to prioritize potential actions at December meeting
- PCI SSC will communicate resulting actions with PCI Community as part of 2025 engagement activities