

# Seismic Change or a Mere Ripple: Changes to Reporting for PCI DSS v4.0

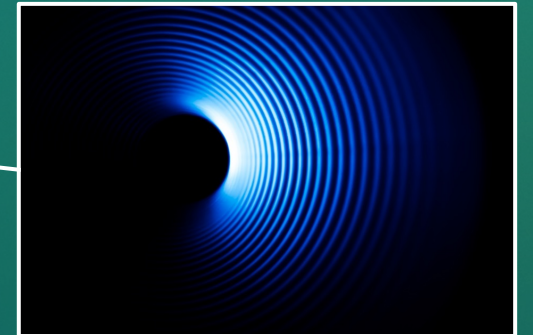
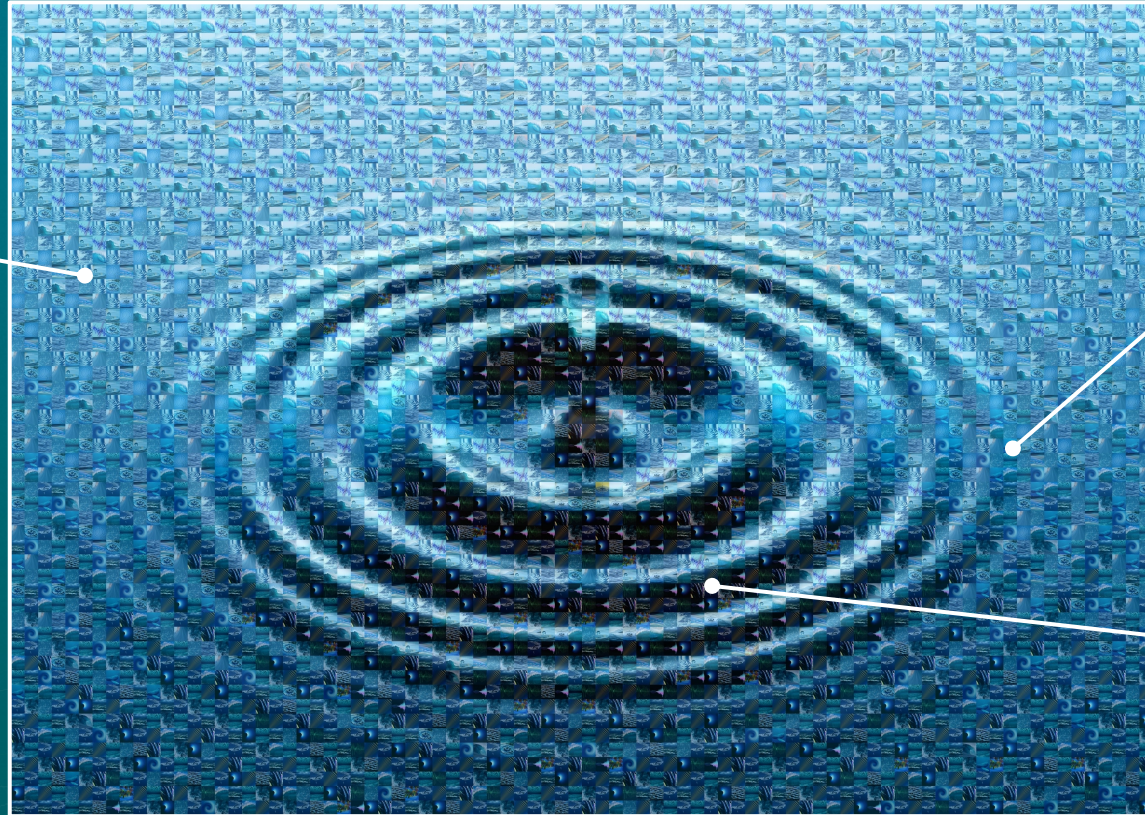
Tracey Long, VP, Programs PCI Security Standards Council  
John Bloomfield, Manager, Data Security Standards  
PCI Security Standards Council





**Navigating the  
(Sometimes)  
Rough Waters**

# Reporting: Telling the Story of the Assessment



# Reporting: Telling the Story of the Assessment (cont'd)



DESCRIPTION OF CDE

PCI Security Standards Council

Payment Card Industry  
Data Security Standard

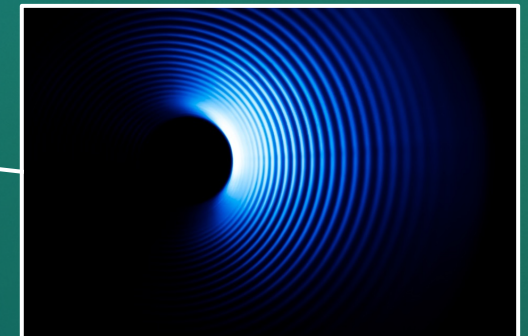
Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (*select one*):

**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby (*Merchant Company Name*) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

Attestation of Compliance for Report  
on Compliance - Merchants  
Version 4.0  
Publication Date: March 2022



EVIDENCE




OPPORTUNITIES FOR  
IMPROVEMENT

# Security as a Continuous Process



BETTER ON-GOING  
SECURITY HYGIENE  
NEEDED



**Payment Card Industry  
Data Security Standard**

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document (*select one*):

**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with Remediation, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby (*Merchant Company Name*) has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.

**Attestation of Compliance for Report  
on Compliance - Merchants**  
Version 4.0  
Publication Date: March 2022



IDENTIFIED ISSUES  
THAT COULD BECOME  
NON-COMPLIANT



REPEAT ENDINGS



**People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems**



**- Cybersecurity Expert Bruce Schneier**  
from *Secrets and Lies: Digital Security in a Networked World*, 2000

# Citation of Workpaper Evidence vs. Narrative Summary

- Less narrative, more reliance on citation of workpaper evidence

| PCI DSS Requirement   |                           |                          |                          |                          |
|---|---------------------------|--------------------------|--------------------------|--------------------------|
| 1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.   |                           |                          |                          |                          |
| Assessment Findings<br>(select one)   |                           |                          |                          |                          |
| In Place  | In Place with Remediation | Not Applicable           | Not Tested               | Not in Place             |
| <input type="checkbox"/>  | <input type="checkbox"/>  | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Describe why the assessment finding was selected.<br><i>Note: Include all details as noted in the "Required Reporting" column of the table in Assessment Findings in the ROC Template Instructions.</i> |                           |                          | <Enter Response Here>    |                          |

**“Describe” = tell the story of the compliance you observed in your own words**

# Citation of Workpaper Evidence vs. Narrative Summary (cont'd)

Less narrative, more reliance on citation of workpaper evidence

| Testing Procedures   | Reporting Instructions   | Reporting Details:<br>Assessor's Response |
|--|--|---|
| <b>1.1.2.a</b> Examine documentation to verify that descriptions of roles and responsibilities for performing activities in Requirement 1 are documented and assigned.             | Identify the evidence reference number(s) from Section 6 for all <b>documentation</b> examined for this testing procedure. | <Enter Response Here>                     |
| <b>1.1.2.b</b> Interview personnel responsible for performing activities in Requirement 1 to verify that roles and responsibilities are assigned as documented and are understood. | Identify the evidence reference number(s) from Section 6 for all <b>interview(s)</b> conducted for this testing procedure. | <Enter Response Here>                     |

**“Identify the evidence” = no story, just reference number(s) from Section 6 Evidence (Assessment Workpapers)**

# Workpaper Evidence Retention: A Reminder

Workpaper evidence must be retained and available for three (3) years,

## 6 Evidence (Assessment Workpapers)

### 6.1 Evidence Retention

|   |  |
|---|--|
| Describe the repositories where the evidence collected during this assessment is stored including the names of the repositories and how the data is secured.  | <Enter Response Here>                                    |
| Identify the entity or entities who controls the evidence repositories.   | <Enter Response Here>                                    |
| Indicate whether the entity or entities in control of the evidence repositories understands that all evidence from this assessment must be maintained for a minimum of 3 years and must be made available to PCI SSC upon request | <input type="checkbox"/> Yes <input type="checkbox"/> No |

Section 6 Evidence (Assessment Workpapers) acknowledges that evidence can be retained by the assessor company or the assessed entity, but still must be made available to PCI SSC upon request. Assessors and entities should plan accordingly

# Additional Reporting Options



Customized approach is optional, so you choose whether it's a ripple or tsunami of change!

- **Customized Approach (ROC only)**

| Validation Method – Customized Approach   |  |
|---|--|
| Indicate whether a Customized Approach was used:  | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| If “Yes”, Identify the aspect(s) of the requirement where the Customized Approach was used.<br><i>Note: The use of Customized Approach must also be documented in <a href="#">Appendix E</a>.</i> | <Enter Response Here>                                    |

# Additional Reporting Options



Customized approach is optional, so you choose whether it's a ripple or tsunami of change!

- **Customized Approach (ROC only)**

| Validation Method – Customized Approach   |  |
|---|--|
| Indicate whether a Customized Approach was used:  | <input type="checkbox"/> Yes <input type="checkbox"/> No |
| If “Yes”, Identify the aspect(s) of the requirement where the Customized Approach was used.<br><i>Note: The use of Customized Approach must also be documented in <a href="#">Appendix E</a>.</i> | <Enter Response Here>                                    |

# Additional Reporting Options



Partial Assessment: New version 4.0 option when there are Not Tested requirements

## • Partial vs full assessment

- Partial could be used for Prioritized Approach
- Could be used for specialized practices/offerings
- See FAQ 1331: Can SAQ eligibility criteria be used for determining applicability of PCI DSS requirements for onsite assessments?



# Let's get into SAQs...



Self-Assessment Questionnaires in PCI DSS v4.0

Validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.



# Let's get into SAQs...



Self-Assessment Questionnaires in PCI DSS v4.0

Validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- SAQ D Service Provider
- SAQ P2PE



# Let's get into SAQs...



Self-Assessment Questionnaires in PCI DSS v4.0

Validation tools for merchants and service providers that are eligible to evaluate and report their PCI DSS compliance via self-assessment.

- **SAQ A**
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- **SAQ D Service Provider**
- SAQ P2PE



# SAQ A



Card-not-present merchants outsourcing to PCI DSS compliant third parties

## Existing Requirements added

- External Vulnerability Scans
- Identifying and Managing Vulnerabilities
- Policies and procedures for the protection of stored account data

## New Requirements added

- Managing all payment page scripts
- Tamper detection for payment pages



# SAQ A



Card-not-present merchants outsourcing to PCI DSS validated and compliant third parties

## Existing Requirements added

- **External Vulnerability Scans**
- **Identifying and Managing Vulnerabilities**
- Policies and procedures for the protection of stored account data

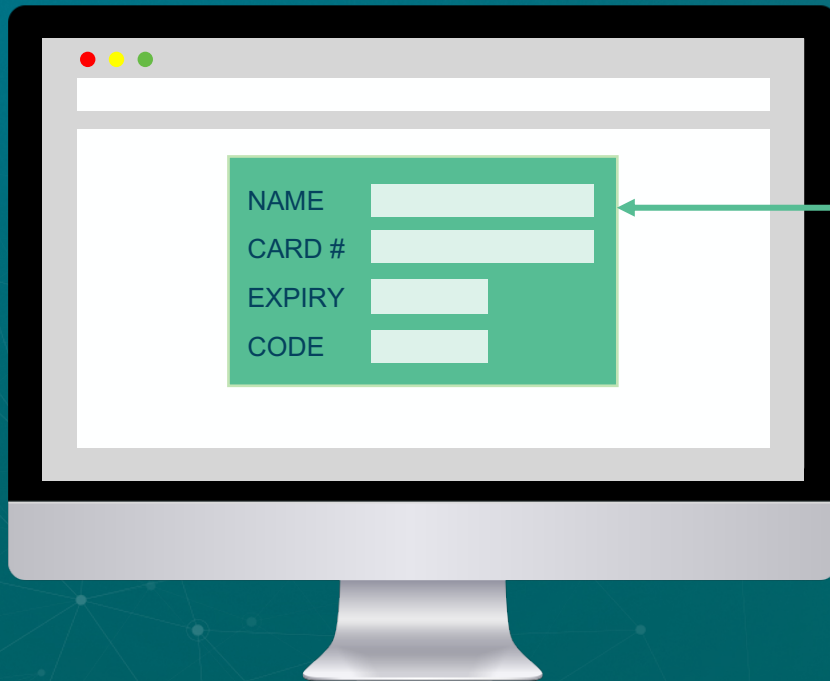
## New Requirements added

- **Managing all payment page scripts**
- **Tamper detection for payment pages**

# SAQ A – Why the New Requirements?



Mitigating risks for ecommerce environments



PCI DSS compliant third-party service provider (TPSP) / payment processor

# SAQ A – Why the New Requirements?



Mitigating risks for ecommerce environments



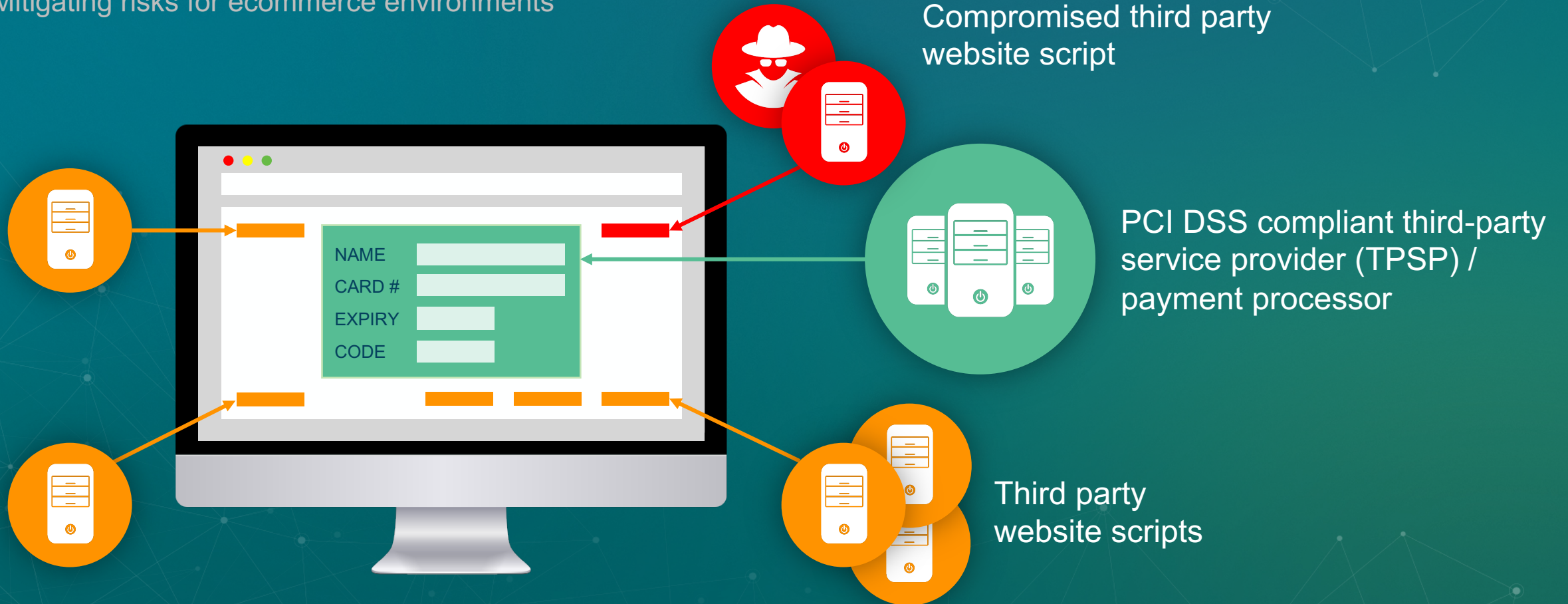
PCI DSS compliant third-party service provider (TPSP) / payment processor

Third party website scripts

# SAQ A – Why the New Requirements?



Mitigating risks for ecommerce environments



# SAQ D – Service Providers



Which SAQ should I select as service provider?

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- SAQ D Service Provider
- SAQ P2PE



# SAQ D – Service Providers



Which SAQ should I select as service provider?

- SAQ A
- SAQ A-EP
- SAQ B
- SAQ B-IP
- SAQ C
- SAQ C-VT
- SAQ D Merchant
- **SAQ D Service Provider**
- SAQ P2PE



**“There can be only one...”**

# SAQ D – Service Provider



What are the big changes in SAQ D – Service Provider?

SAQ D  
Service Provider



- Service Provider Specific Requirements
- Reporting Sections
- Narrative Text

# SAQ Development



How are SAQs developed?

- Define eligibility criteria
- Focus on specific use cases
- Address payment threats



# Future of SAQs



**So...**

**Seismic  
Change  
or a  
Ripple?**

**That's up  
to you!**