



BUREAU OF THE

Fiscal Service

U.S. DEPARTMENT OF THE TREASURY

Card Acquiring Service (CAS) Security Posture and Compliance

May 20, 2020

Housekeeping

Guidelines of today's session

- This webinar has been **pre-recorded**
- To comply with the rules outlined by Treasury's Legislative and Public Affairs Division, no presenter(s) will disclose their identities.
- Please submit all questions to the CAS Outreach Mailbox
 - CardAcquiringService@fiscal.treasury.gov
 - Title SUBJECT LINE as: **CAS PCI Webinar Question**
 - Please provide your **name and agency** in the body of the email.

Purpose: **Why are you here?**

Objectives:

- To educate agencies on data security posture while delivering the necessary compliance rules and regulations around the Payment Card Industry Data Security Standards (PCI DSS) for compliance.

How:

- Supplying agencies with a high-level synopsis of the security Card Acquiring Service (CAS) policies and procedures, outlined in the Treasury Financial Manual (7000) Volume 1, Part 5: Credit and Debit Transactions
- Providing an overview of the CAS Security Posture
- Help our participants with understanding the details of PCI DSS compliance
- Delivering an overview of the certification and security tool, *Trustwave*.



BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Security Posture & PCI DSS

Policies: **CAS governing policies**

What is the Treasury Financial Manual (TFM)?

- The TFM is the Department of the Treasury's (Treasury's) official publication of policies, procedures, and instructions concerning financial management in the Federal Government.

What are the CAS Card Rules?

- The card rules apply to federal agencies that are collecting or intend to collect obligations via credit or debit card. In addition to these requirements, an agency also must comply with and be bound by the rules and regulations governing all debit and credit card transactions accepted by the agency (collectively, the Network Rules), any of which may be altered or amended periodically and without notice.

Policies: **Understanding the CAS Card Rules**

- **Security**

- Section 7065: Retention and Storage of Card Data/Payment Card Industry Data Security Standard

Agencies are subject to requirements, including the Payment Card Industry Data Security Standard and the data retention requirements set forth in the Network Rules.

Agencies that fail to comply with the requirements of this section may be subject to network fines, and/or penalties, liabilities, or damages arising under federal law.

Security is IMPORTANT, ensure your agency is COMPLIANT.

Card Security 101: **Security Posture**

What is a Security Posture? A consistent standard of cardholder data protection across a given footprint.

Drafting the Posture

- Establish minimum standards
- Create the posture

Establishing the Posture

- Align customer agencies data security structure
- Provide understanding of security measures

Implementing the Posture

- Ideal end-state of security posture standards for agency adoption
- Identifying the 4 security posture elements

Card Security 101: Posture Elements

OUR MISSION:

Ensure our agency customers are utilizing a consistent standard of security for cardholder data protection

PCI Compliance

Payment Card Industry Data Security Standard (PCI-DSS):

Is an information security standard for organizations that handle branded credit cards from the major card schemes

EMV
is a payment method based upon a technical standard for smart payment cards and terminals

TOKENIZATION
is the process of substituting a sensitive data element with a non-sensitive equivalent

ENCRYPTION
is the process of encoding a message of information

Merchant Processor Disclosure: **Worldpay**

The information included in this presentation is for information purposes only, and is not intended as legal or financial advice. The information does not amend or alter your obligations under your agreement with Worldpay (formally known as Vantiv), or under the operating regulations of any credit card or debit card association.

This presentation is based upon information available to Worldpay (formally known as Vantiv), as of the date of this communication. It is important that you continue to stay current with changing industry requirements.

PCI DSS: Who does it apply to?

PCI DSS Requirements

- Applies to all organizations, systems, networks and applications that process, store or transmit at least the cardholder number.



- Store no cardholder data beyond name, number, expiration date and service code.

All merchants are required to comply regardless of size!

This includes all U.S. Treasury Agencies that accept cards for payment – even those using Pay.gov!

PCI DSS: High Level Overview

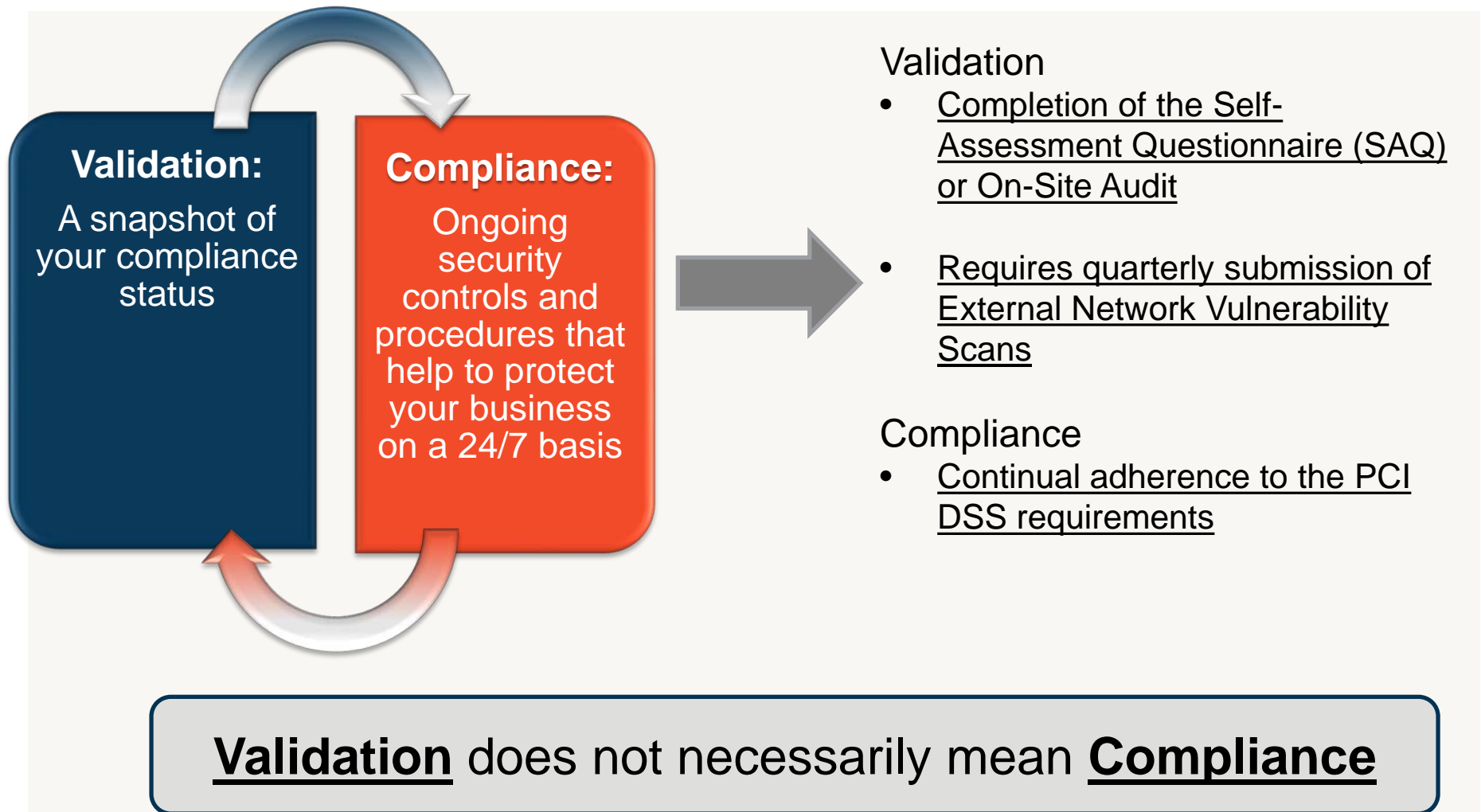
| | |
|--|--|
| Build and Maintain a Secure Network and Systems | <ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system password and other security parameters |
| Protect Cardholder Data | <ol style="list-style-type: none">3. Protect stores cardholder data4. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | <ol style="list-style-type: none">5. Protect all systems against malware and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | <ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Identify and authenticate access to system components9. Restrict physical access to cardholder data |
| Regularly Monitor and Test Networks | <ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes |
| Maintain an Information Security Policy | <ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel |



BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Compliance Validation Steps

PCI DSS: Compliance vs. Validation



Visa & MasterCard Merchant Levels:

Merchant * Level 1

Any merchant processing 6 million or more Visa® or MasterCard® transactions/year, regardless of acceptance channel. Also, any merchant the card brands deem Level 1.

Merchant Level 2

Any merchant, regardless of acceptance channel, processing 1-6 million Visa® or MasterCard® transactions per year

Merchant Level 3

Any merchant processing 20,000 to 1 million e-commerce Visa® or MasterCard® transactions per year

Merchant * Level 4

All other merchants, regardless of acceptance channel

**Level 1 merchants have more rigorous compliance validation requirements.*

**Level 4 merchants also have compliance requirements.*

Merchant Validation: **How does it happen?**

| Merchant Levels | On-Site Assessment | Self-Assessment Questionnaire | Network Vulnerability Scans |
|-----------------|--|---------------------------------|--|
| Level 1 * | Report on Compliance (ROC)* Submitted Annually | Not Applicable | Required Quarterly |
| Level 2 * | Not Applicable | Submitted to Acquirer Annually* | Required Quarterly |
| Level 3 | Not Applicable | Submitted to Acquirer Annually | Required Quarterly |
| Level 4 | Not Applicable | Submitted to Acquirer Annually | Required Quarterly Submitted at Acquirer's Discretion |

*Note: Due to MasterCard® Site Data Protection (SDP) program rules, all level 1 and 2 merchants that elect to perform their own validation assessments must ensure that the primary internal auditor staff engaged in validating PCI DSS compliance attend merchant training programs offered by the PCI Security Standards Council (PCI SSC) and pass any PCI SSC associated accreditation program annually in order to continue validation in this manner.

Self-Assessment Questionnaires (SAQ)

| SAQ | Description |
|--------------|--|
| A | <p>Card-not-present merchants (e-commerce or mail/telephone-order) that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.</p> <p><i>Not applicable to face-to-face channels.</i></p> |
| A-EP* | <p>E-commerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises.</p> <p><i>Applicable only to e-commerce channels.</i></p> |
| B | <p>Merchants using only:</p> <ul style="list-style-type: none"> • Imprint machines with no electronic cardholder data storage; and/or • Standalone, dial-out terminals with no electronic cardholder data storage. <p><i>Not applicable to e-commerce channels.</i></p> |
| B-IP* | <p>Merchants using only standalone, Pin Transaction Security (PTS)-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage.</p> <p><i>Not applicable to e-commerce channels.</i></p> |

**New for PCI DSS v3.0*

Self-Assessment Questionnaires (SAQ)

| SAQ | Description |
|----------------|---|
| C-VT | <p>Merchants who manually enter a single transaction at a time via a keyboard into an Internet-based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage.</p> <p><i>Not applicable to w-commerce channels.</i></p> |
| C | <p>Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.</p> <p><i>Not applicable to e-commerce channels.</i></p> |
| P2PE-HW | <p>Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage.</p> <p><i>Not applicable to e-commerce channels.</i></p> |
| D | <p>SAQ D for Merchants: All merchants not included in descriptions for the above SAQ types</p> |
| | <p>SAQ D for Service Providers: All service providers defined by a payment brand as eligible to complete a SAQ.</p> |

**New for PCI DSS v3.0*



BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Trustwave - PCI Assist

PCI Assist: **What is it?**

- PCI Assist is a set of online data security tools targeted to **Level 4 merchants**
 - Helps merchants protect their businesses with best practices
 - Provides step-by-step instructions for completing critical steps required for PCI compliance validation
- A service provided by Trustwave[®], a leading provider of PCI DSS compliance services
 - Uses Trustkeeper[®] compliance management software



PCI Assist: **Product Features**



- PCI Assist is accessed through Trustwave's portal
 - <https://pci.trustwave.com/fiscalservice>
- Includes self-assessment wizard
- Completes the appropriate SAQ in the background
- Includes an external vulnerability scan for IP connected merchants

Remember:

Cardholder data security is a **merchant's responsibility.**

Level 4 merchants **must validate** compliance annually.

Trustwave: **Registration Details**


- Trustwave Registration - To register you will need:
 1. Company Name
 2. Chain Legal Name
 - If you do not have this, call the Federal Agency Support line at **1-866-914-0558** and request the associated with your account
 3. One of your Merchant ID numbers.
- To get started with Trustwave, please visit:
 - <https://pci.trustwave.com/fiscalservice>



BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Service Providers

Third-Party Compliance



Requirement 12.8 – Addresses Third-Party compliance within PCI DSS requirements

Merchant is responsible for monitoring compliance status of Third Parties and ensuring the use of appropriate contractual language

Use of Gateway/Service Provider does not exempt merchant from compliance requirements

Potential to use SAQ A

- **Only IF** all storing, processing and transmitting of cardholder data is fully outsourced to a third party AND merchant is **exclusively** card-not-present.

Service Provider Validation

| Service Provider Levels | Validation Actions | | |
|--|--|---------------------------------|----------------------------------|
| Criteria | On Site Security Audit conducted by a QSA | Self – Assessment Questionnaire | Network Vulnerability Scans |
| <p>Level 1</p> <p>Any processor directly connected to a Visa or MasterCard or any service provider that stores, processes and/or transmits over 300,000 transactions per year</p> | <p>Report on Compliance (ROC)</p> <p>Required Annually</p> | <p>Not Applicable</p> | <p>Required Quarterly</p> |
| <p>Level 2**</p> <p>Any service provider that stores, processes and/or transmits less than 300,000 transactions per year</p> | <p>Not Applicable</p> | <p>Required Annually</p> | <p>Required Quarterly</p> |

**Effective February 1, 2009, Level 2 service providers were no longer listed on Visa's List of PCI DSS Compliant Service Providers. Entities that wish to be on the List of PCI DSS Compliant Service Providers must validate as a Level 1 provider.

Service Provider: **Considerations**

- Where possible, use only providers that have engaged a QSA for validation.
- If you have a **Level 2** service provider that self validates, only accept SAQ D.
- Their areas of non-compliance are your risk.
- If a provider states they cannot afford some aspect of compliance or validation, you may want to consider one that can.
- Carefully review your contracts with service providers.

Webinar Recap: **What have you learned?**

Educate

Delivered understanding of TFM, Chapter 7000, Section 7065 on PCI DSS

Supplied overview of the CAS Security Posture

Provided informational overview of *Trustwave*



Implement

Ensure all devices follow the CAS Security Posture

Make sure card information is being stored properly and all holding systems are PCI DSS compliant.



BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

Next Steps

Next Steps - **What's up next?**

1

We are asking participants to refresh themselves with the TFM, <https://tfm.fiscal.treasury.gov/v1/p5/c700.html>

2

Complete the post-webinar survey

3

Submit questions to the CAS Outreach Mailbox
(CardAcquiringService@fiscal.treasury.gov)

Upcoming Webinars: **Save the Date**





BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

QUESTIONS?

Submit questions via the CAS Outreach Mailbox
CardAcquiringService@fiscal.treasury.gov

Contact Information



CAS Agency Outreach Mailbox

CardAcquiringService@fiscal.treasury.gov

ARM Mailbox

ARM@fiscal.treasury.gov

For More Information

CAS Online: www.fiscal.treasury.gov/cas



BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

APPENDIX

Appendix A - **TFM References**

Section 7065—Retention and Storage of Card Data/Payment Card Industry Data Security Standard

- 7065.20—Payment Card Industry Data Security Standard (PCI DSS)

Section 7090—CAS Program Non-Compliant Notice and Suspension of Service Process

Appendix B - **Glossary**

ARM – Agency Relationship Management

CAS – Card Acquiring Service

CASA – Card Acquiring Service Application

CIR – Collections Information Repository

PCI DSS – Payment Card Industry Data Security Standards

TFM – Treasury Financial Manual

SSD – Settlement Services Division

Appendix C - **Helpful PCI Resources**

- **PCI Security Standards Council – www.pcisecuritystandards.org**
 - PCI DSS, PA DSS, PTS, & P2PE Standards
 - Downloadable Self Assessment Questionnaires
 - List of ASVs, QSAs, PFIs, PA QSAs, QIRs, etc.
 - List of PA DSS Validated Payment Applications, validated P2PE solutions, validated PTS devices
 - Searchable FAQ Tool
 - PCI Supporting Documents
- **Visa® CISP website – www.visa.com/cisp**
 - Merchant & Service Provider Levels Defined
 - List of CISP Compliant Service Providers
 - Important Alerts, Bulletins and Webinar
- **MasterCard® SDP website – www.mastercard.com/sdp**
 - Merchant & Service Provider Levels Defined
 - List of CISP Compliant Service Providers
 - PCI 360 Merchant Education Program – on demand educational webinars