Office of the Treasurer-Tax Collector
SHARI L. FREIDENRICH, C.P.A.

HALL OF FINANCE & RECORDS
625 N. ROSS STREET, BUILDING 11, ROOM G-76
POST OFFICE BOX 4515
SANTA ANA, CA 92702-4515
www.ttc.ocgov.com

Treasurer Procedures Manual
Treasurer-Tax Collector, County of Orange

SUBJECT: Payment Card Industry Data Security Standards Policy		NUMBER: 9.0
APPROVED BY: Shari L. Freidenrich		EFFECTIVE DATE: 01/10
TITLE: Treasurer-Tax Collector	DATE SIGNED: 02/01/13	DATE REVISED: 02/13

I. Policy

This policy is not intended to replace Payment Card Industry Data Security Standards (PCI DSS). Agencies that accept credit card transactions should use this as a guide to ensure compliance with PCI DSS. Revisions to the PCI DSS could occur at any time. The current version of PCI DSS is 2.0 and was published in October 2010. The next revision of PCI DSS is expected to be published around October 2013. For the latest in PCI DSS information please visit the PCI website at: www.pcisecuritystandards.org.

A. Overview

In order to protect cardholder information and maintain compliance with the Payment Card Industry Data Security Standards (PCI DSS), any agency (merchant) within the County of Orange (County) that processes credit card transactions must comply with PCI Data Security Standards by completing the PCI DSS Compliance Validation Requirements. These requirements consist of completing a Self Assessment Questionnaire (SAQ), submitting an Attestation of Compliance (AOC) and if applicable, performing a quarterly network scan. On an annual basis, around January or February, merchants should review credit card transaction activity for the previous calendar year. PCI DSS Compliance Validation Requirements must be completed by April 30 of each year based on the activity from the previous year.

The PCI Security Standards Council (PCI SSC) (founded by the five major card associations: Visa, MasterCard, American Express, Discover, JCB) established a set of rules that require merchants and third party vendors who store or transmit cardholder data on behalf of the merchant to adhere to PCI Data Security Standards. These standards are intended to assist in fraud prevention by protecting cardholder data.

Failure to comply with PCI Data Security Standards can result in losing the ability to process card payments. Card associations may also impose hefty fines as a result of

non-compliance or breach in cardholder information. Failure to comply with these standards may also result in a violation of federal or state law.

Included in this document, you will find a glossary and links to various resources to further explain PCI DSS. While PCI DSS compliance is the responsibility of each merchant, the overall program is managed by the County Treasurer. Please contact the Treasurer's Cash Management division for further information and documentation, if needed. The current contact is Rosanne Jin at 714-834-4170, rjin@ttc.ocgov.com. **After February 15, 2013, Rosanne will be on leave through August 13, 2013. During this period please contact Kim Hansen at 714-834-5508, khansen@ttc.ocgov.com.**

B. The PCI Data Security Standards

There are twelve fundamental requirements that make up the core of PCI Data Security Standards. Not all requirements apply to every merchant. For locations that use stand-alone dial-up terminals with no cardholder data being transmitted to internal systems or via the Internet, the top five requirements are: 3, 4, 7, 9, and 12 – listed below. For all other locations such as those that handle card-not-present transactions, have payment application systems connected to the Internet, store any portion of cardholder data electronically, or use wireless local area networks (WLAN) each requirement must be met.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data

4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need to know

8. Assign a unique ID to each person with computer access

9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data

11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

II. PCI Compliance Validation Requirements

A. PCI Levels

Merchants are classified into one of the four PCI DSS levels based on card transaction volume over a 12-month period. Each level has defined compliance requirements. There are two compliance guidelines – one for MasterCard and Visa transactions and one for American Express transactions. For MasterCard and Visa transactions, use the highest volume of the two to determine your PCI DSS level. The table below will help to determine your PCI level and what the validation requirements are for that level.

Please note: For the County of Orange, PCI DSS compliance requirements are determined at the location level. Each location within the County of Orange that accepts credit cards is responsible for their own PCI DSS compliance. The TTC will work with you to ensure compliance. If you have questions regarding your PCI DSS level or PCI DSS Compliance, please contact Rosanne Jin from the Treasurer's Office at 714-834-4170, rjin@ttc.ocgov.com. After February 15, 2013, Rosanne will be on leave through August 13, 2013. During this period please contact Kim Hansen at 714-834-5508, khansen@ttc.ocgov.com.

You may also contact our Wells Fargo Merchant Services representative, Glenda Shultz at (301) 745-7002 or you may email her at Glendax.Shultz@WellsFargoMerchantServicesLLC.com.

PCI Level	Visa and MasterCard	American Express	PCI DSS Compliance Validation Requirements
1	• Over 6 million Visa or MasterCard transactions per year • Businesses that experienced a data compromise • Businesses meeting the Level 1 criteria of another payment card brand	• Over 2.5 million American Express transactions per year • Businesses that experienced a data compromise	• Annual onsite review by a qualified Security Assessor • Quarterly network security scan by an Approved Scanning Vendor • Annual submission of a compliant "PCI Report On Compliance" • Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only
2	• 1 million to 6 million Visa or MasterCard transactions per year • Businesses meeting the Level 2 criteria of another payment card brand	• 50,000 to 2.5 million American Express transactions per year	• Annual Self Assessment Questionnaire • Quarterly network security scan by an Approved Scanning Vendor • Annual signed "Attestation on Non-Storage of Non-Compliant Data" for non-compliant businesses only • Annual signed "Attestation of Report Accuracy"
3	• 20,000 to 1 million e-commerce Visa or MasterCard transactions per year	• N/A	• Annual Self Assessment Questionnaire • Quarterly network security scan by an Approved Scanning Vendor • Annual signed "Attestation of Report Accuracy"
4	• All other businesses	• All other businesses • This is considered Level 3 for American Express but compares to V/MC Level 4 requirements	• Annual Self Assessment Questionnaire • Quarterly network security scan by an Approved Scanning Vendor strongly recommended

B. Self Assessment Questionnaires (SAQ)

The SAQ is a document intended to assist merchants in self-evaluating their compliance with the PCI DSS. There are six SAQ validation categories, shown briefly in the table below and described in more detail in the Self Assessment Questionnaire Instruction Guide. Use the table to gauge which SAQ applies to your location, then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

Current copies of each SAQ as well as the Instruction Guide are available on the PCI SSC Website:

https://www.pcisecuritystandards.org/security_standards/documents.php?category=saqs

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage. *This would never apply to e-commerce merchants.*
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage. *This would never apply to e-commerce merchants.*
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.
D	All other merchants not included in descriptions for SAQ types A through C above, and **all service providers** defined by a payment brand as eligible to complete an SAQ.
P2PE-HW	Merchants using only hardware payment terminals included in a PCI SSC-listed, validated, P2PE solution, no electronic cardholder data storage. *This would never apply to e-commerce merchants.*

****Important Note:**
SAQ's and a signed Attestation of Compliance must be submitted to the Cash Management Division of the Treasurer's office by April 30th of each year. Scanned, electronic copies should be emailed to Cash Management at cashmgmt@ttc.ocgov.com. Failure to comply could result in the closure of your merchant account.

For locations that use Wells Fargo Bank as their merchant bank, the Treasurer's Office will submit the SAQ and signed Attestation of Compliance to Wells Fargo.

For locations that use a merchant bank other than Wells Fargo Bank, SAQ's and the signed Attestation of Compliance will be maintained by the Treasurer's office and submitted to the appropriate areas. The TTC will coordinate with these departments so TTC can submit the forms to their merchant bank. Please keep in mind, the use of merchant banks outside Wells Fargo must be reviewed and approved in advance by the Treasurer's Office.

C. Approved Scanning Vendors (ASV)

Depending on your PCI DSS level, quarterly network security scans may be required by an ASV. ASVs are organizations that validate adherence to certain PCI DSS requirements by performing vulnerability scans of internet facing environments of merchants and service providers. A list of ASVs certified by PCI SSC can be found at:
https://www.pcisecuritystandards.org/pdfs/asv_report.html

In order to perform a network scan, agencies will need to work with their IT resources to make sure that the correct external IP addresses for merchant card processing are identified. In addition, CEO IT has asked the agency's IT resources to notify them of the date and time that the scan will be performed by opening a HELPDESK ticket 3-5 days prior to the scan. This is needed to avoid agency network access shut down if their system detects a threat. During the scan, IT should monitor the agency's systems to ensure other business systems are not impacted.

D. Wells Fargo Merchant Services Trustwave Program

Some County of Orange locations are required to participate in a specific PCI DSS compliance program through Wells Fargo Merchant Services. This includes completing the SAQ online and performing quarterly network scans through Wells Fargo's preferred vendor, Trustwave. Non-compliance will result in an additional monthly fee from the bank. Any location that qualifies for this program has already been notified and should be aware of the requirements. The SAQ's for locations enrolled in this program are due one year from the date they were last completed through Trustwave. However, any location that does not complete the SAQ online must adhere to the due date of the County policy. Wells Fargo may identify and enroll additional locations at any time. The Treasurer's Office works closely with Wells Fargo to monitor the compliance of all locations.

III. Third Party Processors

It is the merchant's responsibility to ensure that all applications hosted and/or furnished by a third party processor that receives or processes cardholder data to accept credit card payments comply with PCI Data Security Standards. Contracts with third party processors should require that the vendor be PCI compliant for the entire duration of the contract. In addition, you should request a certificate of compliance annually from your third party processor. Please keep in mind, use of third party processors must be reviewed and approved in advance by the Treasurer's Office.

IV. Software - Payment Application Data Security Standards (PA-DSS)

The PA-DSS certification is for software developers and integrators of payment applications that store, process or transmit cardholder data as part of authorization or settlement when these applications are sold, distributed or licensed to third parties**.**

Effective July 1, 2010, Visa has mandated that any payment application that stores, processes, or transmits cardholder data as part of authorization or settlement MUST be validated and certified as PA-DSS compliant. Failure to use a payment application that is PA-DSS certified will result in the merchant bank ceasing to process credit card payments on your behalf. For more information regarding which applications are eligible for PA-DSS Validation please visit the following fact sheet:

https://www.pcisecuritystandards.org/documents/which_applications_eligible_for_pa-dss_validation.pdf

Validated applications are listed at:
https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

There are fourteen requirements to protecting Payment Application transactions:

1. Do not retain full magnetic stripe, card validation code or value (CAV2, CID, CVC2, CVV2) or PIN block data
2. Provide secure password features
3. Protect stored cardholder data
4. Log application activity
5. Develop secure applications
6. Protect wireless transmission
7. Test applications to address vulnerabilities
8. Facilitate secure network implementation

9. Cardholder data must never be stored on a server connected to the Internet
10. Facilitate secure remote software updates
11. Facilitate secure remote access to applications
12. Encrypt sensitive traffic over public networks
13. Encrypt all non-console administrative access
14. Maintain instructional documentation and training programs for customers, resellers, and integrators

*Note: California state law requires that cardholder expiration dates be masked on **both** the merchant and customer receipts. This is not a PCI DSS requirement; however, it is equally important (California Civil Code § 1747.09).

V. Hardware – Payment Card Devices

Any device used to swipe cards must encrypt the data at the point of capture.

Any pin pad device must comply with the PCI personal identification number (PIN) entry device (PED) security requirements (PCI PED).

VI. Mobile Payments – Point-to-Point Encryption (P2PE)

Many merchants seek innovative ways to engage customers and improve the payment experience. The ever-expanding capabilities of mobile devices such as smart phones or tablets now includes payment acceptance. Along with the increased convenience at the Point of Sale, mobile payment acceptance can also bring new risks to the security of cardholder data. Securing account data at the point of capture is one way that you can actively help in controlling these risks. Validated Point-to-Point Encryption (P2PE) solutions will be listed on the PCI Council (PCI SSC) website, however, currently the information is not yet available. If you choose to accept mobile payments, these solutions may help you in your responsibilities under PCI DSS. For more information regarding P2PE, please click on the following link:

https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf

VII. Resources

For current information regarding PCI DSS, please visit the **PCI Security Standards Council's website at:**
https://www.pcisecuritystandards.org/

For additional information regarding PCI Compliance, please visit:
http://www.pcicomplianceguide.org/

For the current version of a **PCI Quick Reference Guide**, please visit the link below:
https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf

For **PCI DSS v2.0** please visit the link below:
https://www.pcisecuritystandards.org/security_standards/documents.php

For the **PCI DSS Glossary**, please visit:
https://www.pcisecuritystandards.org/security_standards/glossary.php

For the current version of the **Navigating PCI DSS** document, please visit the link below:
https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf

For current versions of the **SAQ, Attestation of Compliance and SAQ Instruction** documents, please visit the link below and click on the tab called SAQs:
https://www.pcisecuritystandards.org/security_standards/documents.php

For current versions of the **Prioritized Approach to Pursue PCI DSS Compliance** and the associated **Release Notes and Instructions**, please visit the link below:
https://www.pcisecuritystandards.org/documents/Prioritized_Approach_PCI_DSS_1_2.pdf

For current list of **Approved Scanning Vendors (ASV)**, please visit the link below:
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

For current list of **Payment Application Data Security Standards (PA DSS)** certified vendors, please visit the link below:
https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php

For more information regarding **Mobile Payments and P2PE**, please click on the links below:
https://www.pcisecuritystandards.org/documents/accepting_mobile_payments_with_a_smartphone_or_tablet.pdf

http://www.pcicomplianceguide.org/docs/PCI_SSC_P2PE_Update_July_2012.pdf

Additional Resources:

Visa Business Guide to Data Security
https://usa.visa.com/merchants/risk_management/data_security_demo/popup.html

MasterCard PCI 360
www.mastercard.com/pci360

Wells Fargo Bank – Merchant Compliance
https://www.wellsfargo.com/biz/merchant/service/manage/risk/security

VIII. Glossary

Application – Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications

Cardholder – Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.

Cardholder Data – At a minimum, cardholder data contains the full primary account number (PAN) or full magnetic stripe data. Cardholder data may also appear in the form of the full primary account number plus any of the following:

- Cardholder name
- Expiration date
- Service Code

Card Validation Code or Value – Refers to either: (1) magnetic-stripe data or (2) printed security features:

(1) Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV or CSC pending on payment card brand. The following list provides the terms for each card brand:

- **CAV –** Card Authentication Value (JCB payment cards)
- **CVC –** Card Validation Code (MasterCard payment cards)
- **CVV –** Card Verification Value (Visa and Discover payment cards)
- **CSC –** Card Security Code (American Express)

(2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit un-embossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with

each individual card and ties the Primary Account Number (PAN) to the card. The following provides an overview:

- **CID –** Card Identification Number (American Express and Discover payment cards)
- **CAV2 –** Card Authentication Value 2 (JCB payment cards)
- **CVC2 –** Card Validation Code 2 (MasterCard payment cards)
- **CVV2 –** Card Verification Value 2 (Visa payment cards)

Headquarter – a parent number assigned to one or more merchant IDs as a way to group similar operating locations.

Location – Refers to each County of Orange agency that processes card transactions assigned with their own unique headquarter.

Magnetic-Stripe Data – Also referred to as "track data". Data encoded in the magnetic stripe or chip used for authorization during payment transactions. Can be the magnetic stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe. Entities must not retain full magnetic stripe data after obtaining transaction authorization.

Masking – Method of concealing a segment of data when displayed. Masking is used when there is no business requirement to view the entire PAN.

Merchant – any location that processes credit card payments.

Merchant Identification (MID) – A number assigned to each merchant identifying each merchant.

PAN – Acronym for "primary account number" and also referred to as "account number." The PAN is the account number printed on the front of a payment card.