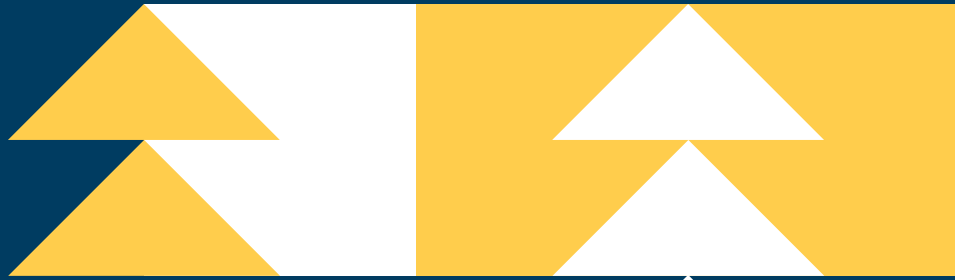




**OREGON
STATE
TREASURY**



Inside the Vault

State Agency Edition

Payment Card Industry

Data Security Standard Forum

On Tuesday, September 24, Treasury is hosting a forum on the Payment Card Industry Data Security Standard (PCI DSS) in Salem for agencies that accept merchant cards. Representatives from U.S. Bank/Elavon and a PCI DSS Qualified Security Assessor will present information about the PCI DSS version 3.2.1. U.S. Bank/Elavon also will demonstrate their PCI Compliance Manager solution, which agencies can utilize to validate compliance with the PCI DSS. Treasury staff will review agency responsibilities for compliance with the PCI DSS and will preview a new Treasury policy that consolidates existing compliance requirements and outlines new service options available to agencies, *e.g.*, Elavon's PCI Compliance Manager.

(Continued on page 2)



Upcoming Holiday

Monday, October 14, is Columbus Day. While Treasury will be open, the Federal Reserve and Oregon banks will be closed. Due to the closures, no incoming ACH or redeemed check information will be distributed on October 14. In addition, ACH files sent to Treasury by STAN agencies for processing on Friday, October 11, must have an effective date of Tuesday, October 15, or later. STAN Online will be unavailable from 1:00 p.m. Friday, October 11, to 1:00 p.m. Monday, October 14. ACH files sent to Treasury via FTP between 10:00 a.m. Friday, October 11, and 10:00 a.m. Tuesday, October 15, must have an effective date of Wednesday, October 16, or later.

Interest Rates

Average Annualized Yield

July	2.75%
August	2.6387%

Interest Rates

July 1–August 8	2.75%
August 9–31	2.60%

(Continued from page 1)

Who Should Attend?

- ▶ Business and IT Managers responsible for overseeing the financial controls relevant to the PCI DSS within your organization.
- ▶ Business and IT staff who are responsible for completing the PCI DSS Self-Assessment Questionnaires.
- ▶ Others that may have a role in PCI DSS compliance and awareness.

About the PCI DSS

Merchant cards—or credit and debit cards—are the lifeblood of modern commerce. Customers and businesses alike prefer the convenience that merchant cards offer. And accepting merchant cards can be an efficient way to facilitate electronic payments through all payment channels: point-of-sale, mail order or telephone order, and online. But, merchant card acceptance presents unique security concerns and comes with significant security requirements.



The Payment Card Industry Data Security Standard (PCI DSS) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures associated with credit and debit card account data. The standard was developed by the founding payment card brands of the PCI Security Standards Council in order to facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is intended to help organizations proactively protect customer card account data that is either transmitted, processed, or stored.

Based on selected merchant card processing methods, agencies are required to establish and maintain a proper security environment to safeguard customer payment information at all times. At a minimum, agencies must maintain compliance with PCI DSS requirements.

Learn more about the PCI DSS and how your agency can protect itself and its customers. Registration closes at 5:00pm this Friday, so [sign up](#) today!

ACH and Merchant Card Risk Assessments

The annual deadline for completion of ACH Risk Assessments is December 31. Treasury will send reminders and instructions about the annual review process by October 5. Those reminders will go to agency ACH contacts. The deadline for Payment Card Industry Data Security Standards (PCI DSS) Self-Assessment Questionnaires (SAQs) will depend on the compliance validation method used by each agency for completion of its annual assessment. More information will be provided after the upcoming PCI DSS forum. We appreciate your ongoing efforts in protecting your customers' sensitive cardholder data and bank account information. If you have any questions about these assessments, please contact Customer Solutions at customersolutions@ost.state.or.us.



Service Spotlight

E-commerce is the selling or purchasing of goods and services online. And because the exchange takes place online, there are two primary payment methods that can be used. The first is the use of a merchant card (debit or credit), which requires adherence to the Payment Card Industry Data Security Standard (PCI DSS). The second is the use of bank account and routing information, which ultimately is used to produce an Automated Clearing House (ACH) or “e-check” transaction and requires adherence to the NACHA rules.

Agencies have three options when exploring e-commerce solutions:

- ▶ The OSCIO E-Government Program has contracted with private industry partners to provide statewide e-commerce services. An agency must still complete a work order contract specific to its implementation, but Treasury has qualified both ACH and merchant card options for the E-Government Program.
- ▶ Treasury has contracted with U.S. Bank to provide a solution that supports both ACH and merchant card options.
- ▶ Agencies may follow appropriate procurement processes to contract directly with third party vendors. Treasury must review and approve third party vendors for compliance with Treasury policy FIN 214 and related public funds laws, PCI DSS, and NACHA requirements as may be applicable. Agencies should contact Customer Solutions early in the process to prevent delays.

If you are interested in evaluating your business needs and available options, or have questions about e-commerce solutions generally, contact Customer Solutions at customersolutions@ost.state.or.us.

Merchant Card Class Action Lawsuit

A class action lawsuit has been filed in federal court on behalf of merchants that accepted Visa or Mastercard credit or debit cards between January 1, 2004 and January 25, 2019. The lawsuit is principally about interchange fees charged to merchants. A proposed settlement would provide between \$5.54 billion and \$6.24 billion to class members. As administrator of the statewide Master Agreement for Merchant Card Services, Treasury is working with the Oregon Department of Justice to monitor the lawsuit and coordinate any claim on behalf of the state. If you have received a notice about the Payment Card Interchange Fee Settlement, please contact Customer Solutions at customersolutions@ost.state.or.us.

Director of Finance

Cora Parker
503.378.4633

Deputy Director of Finance

Mike Auman
503.378.2752

Policy & Strategy Manager

Bryan Cruz González
503.378.3496

Cash Management Analyst

Natalya Cudahey
503.378.8256

Administrative Specialist

Kari McCaw
503.378.4633

▲ ▲ ▲

Cash Management

**Improvement &
Renewal Program**
cmirp@ost.state.or.us

Business Analyst

Angel Bringelson
503.378.5865

**Contracted Project Manager
(TEK Systems)**

David Riffle
503.373.7864

Banking Fax

503.373.1179

Banking Operations Manager

Brady Coy
503.378.2457

Banking Operations Coordinator

Ellis Williams
503.378.4990

ACH File Issues

ach.exception.notify@ost.state.or.us

Check Fraud/Stop Payments

Check Image Requests

Check Stock Testing

Ashley Moya
503.373.1944

Fed Wires/ACH Origination

Shannon Higgins
503.378.5043

Local Government Investment Pool

Brady Coy
503.378.2457

Merchant Card/U.S. Bank

Nikki Main
503.378.2409

Online User

Password Resets

ost.banking@ost.state.or.us

Safekeeping/Debt Service

Sherry Hayter
503.378.2895

Customer Solutions Team

customersolutions@ost.state.or.us

**Customer Solutions Regulatory
Manager**

Sharon Prentice
503.373.7312

**Customer Solutions Services
Manager**

Edie Kessel
503.373.1897

Customer Solutions Consultant

Shannon Kammerman
503.378.8562

▲ ▲ ▲

Public Funds Coordinator

Sharon Prentice
503.373.7312

OREGON STATE TREASURY

350 Winter Street NE, Suite 100 ► Salem, OR 97301-3896
oregon.gov/treasury