



WWW.OST.STATE.OR.US  
350 WINTER ST, NE SUITE 100  
SALEM, OREGON 97301

# Inside the Vault

## Cash Management News

OCTOBER 2018

### INSIDE THIS ISSUE

- National Cybersecurity Awareness Month
- Change Agent Network for EFT Project
- Stop.Think.Connect
- Upcoming Holiday
- Service Spotlight
- Data Security Reminder
- E-Payments Routing Directory



### HOLIDAY

**Veterans Day  
November 12**

Treasury Closed  
Banks Closed

*See article for more information*

## NATIONAL CYBERSECURITY AWARENESS MONTH

Protecting your customers' cardholder, bank account, or other sensitive information is a continuous, ongoing process—not a single event or action. Recognizing the importance of cybersecurity awareness, the United States Department of Homeland Security (DHS) has designated October as National Cybersecurity Awareness Month—an annual campaign to raise awareness about cybersecurity. Treasury participates in this national month of awareness by taking the opportunity to remind our customers of the importance of information security.

2018 marks the 15th year of this important effort, which emphasizes that cybersecurity is a shared responsibility and that we all must work together to improve our nation's cybersecurity. Following that theme, this month's newsletter includes a few items related to security practices. While it's important for our agency customers to ensure that your systems are secure, employees continue to be the single biggest threat to sensitive data by opening and/or clicking links in phishing e-mails. More information about National Cybersecurity Awareness Month is available at

<https://www.dhs.gov/national-cyber-security-awareness-month>.

## CHANGE AGENT NETWORK FOR EFT PROJECT

Treasury and KeyBank have spent the past few months working on initial project planning for the Electronic Funds Transfer (EFT) Business Systems Renewal (BSR), which will transform both how we internally operate ACH, wire transfer, and book transfer services and how we deliver those services to our customers. To help those efforts, and to support what is expected to be a multi-year implementation, we will soon begin reaching out to customer agencies to establish a network of change agents. These representatives—including executive leadership, program staff, central services staff, and IT staff—will serve as critical conduits to ensure effective two-way communication and project success.

The EFT BSR is one of the ways the Finance Division is working to transform how we do business while modernizing our operations and technology. Once implemented, the new service delivery model will streamline processing while reducing risk and enhancing service. The effort also will strengthen Treasury's organizational resiliency, allowing us to manage and leverage opportunities that benefit our organization, our customers, and Oregon as a whole.

Contact us at [EFT.BSR@ost.state.or.us](mailto:EFT.BSR@ost.state.or.us) with any questions about the project and look for more information in future issues.

### INTEREST RATE

Average  
Annualized Yield

September  
**2.25 percent**

Interest Rate

September 1–30  
**2.25 percent**

## STOP.THINK.CONNECT

The Department of Homeland Security (DHS) has a number of resources available to the public regarding cyber security. One of those resources is the Stop.Think.Connect campaign, which is a continuous national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. Cybersecurity is a shared responsibility. We each have to do our part to keep the Internet safe. When we all take simple steps to be safer online, it makes using the Internet a more secure experience for everyone.

This October, and every day, follow these simple online safety tips:

- **Enable stronger authentication.** Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media and financial accounts. Stronger authentication (e.g., multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account. For more information about authentication, visit the Lock Down Your Login Campaign at [www.lockdownyourlogin.org](http://www.lockdownyourlogin.org).
- **Make your passwords long and strong.** Use complex passwords with a combination of numbers, symbols, and letters. Use unique passwords for different accounts. Change your passwords regularly, especially if you believe they have been compromised.
- **Keep a clean machine.** Update the security software, operating system, and web browser on all of your Internet-connected devices. Keeping your security software up to date will prevent attackers from taking advantage of known vulnerabilities.
- **When in doubt, throw it out.** Links in email and online posts are often the way cyber criminals compromise your computer. If it looks suspicious (even if you know the source), delete it.
- **Share with care.** Limit the amount of personal information you share online and use privacy settings to avoid sharing information widely.
- **Secure your Wi-Fi network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network, and your digital devices, by changing the factory-set default password and username.

Learn more about the DHS Stop.Think.Connect campaign at <https://www.dhs.gov/stopthinkconnect>.

## UPCOMING HOLIDAY

Due to the Veterans Day holiday, Treasury, the Federal Reserve, and Oregon banks will be closed on Monday, November 12. Customer statements and files will not be produced for November 12 due to the closures. In addition, ACH files sent to the Treasury after the deadline on Friday, November 9, will be sent to the bank on Tuesday, November 13, and must have an effective date of November 14 or later.

## SERVICE SPOTLIGHT

**Safekeeping** is a free service that allows agencies to store items of value in Treasury's vaults. Items placed in safekeeping are usually some form of security being held to insure performance, cover a liability, or provide some other means of financial protection. Items placed in safekeeping are inventoried and agencies receive a receipt for each item. Agencies must submit a written request to retrieve items from safekeeping and items must be picked up in person. If you are interested in safekeeping, or have questions regarding cash management services generally, contact Customer Solutions at [customersolutions@ost.state.or.us](mailto:customersolutions@ost.state.or.us).



## DATA SECURITY REMINDER

It is becoming more commonplace for major retailers, restaurants, or government organizations to announce a data security breach. While each breach is unique, each results in the possibility of data being compromised. Such data can include credit card numbers, bank account information, social security numbers, or other personally identifiable information. Since most agencies transmit, process, or store this same information in electronic or physical format, it is vitally important for agencies to be diligent about keeping data security at the forefront of business decisions and processes.

As a reminder, in addition to the Payment Card Industry Data Security Standard (PCI DSS) and NACHA Rules, agencies are required to comply with Office of the State Chief Information Officer Enterprise Security Office policies, Oregon Accounting Manual Chapter 10, as well as Treasury Cash Management Policies. Please check in with your agency's security team, CFO, or manager responsible for financial controls about the status of your organization's compliance with such requirements as they may reduce the risk of a data breach.

Below are a few recurring themes included in many regulatory requirements that are intended to help safeguard sensitive information:

- Maintain updated data security policies and procedures that are aligned with applicable regulatory requirements.
- Ensure that agency management and staff are aware of your organization's liabilities and responsibilities for protecting sensitive information when processing payments including merchant cards, ACH transactions, and onsite electronic deposits.
- Provide training to staff, at least annually, about the data security policies and procedures applicable to their duties.
- Re-evaluate the reason for storing personally identifiable information.

These are but a few reminders about protecting your customers' personally identifiable information. If you have questions about the regulatory requirements for any of the banking services used by your organization, please contact Customer Solutions at [customersolutions@ost.state.or.us](mailto:customersolutions@ost.state.or.us)



## E-PAYMENTS ROUTING DIRECTORY



The Federal Reserve has announced that the E-Payments Routing Directory will no longer be publicly available on FRBservices.org as of December 9. The directory data files provide basic routing information and Treasury is aware that some agencies use the data files to process transactions. Treasury is working with our financial services providers to explore alternate solutions. If your agency currently uses the directory data files, contact Customer Solutions at [customersolutions@ost.state.or.us](mailto:customersolutions@ost.state.or.us) to discuss your needs.

## CONTACT INFORMATION

**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

**Administrative Specialist**

Kari McCaw  
(503) 378-4633

◆◆◆

**Cash Management  
Improvement &  
Renewal Program**

[cmirp@ost.state.or.us](mailto:cmirp@ost.state.or.us)

**Business Analyst**

Angel Bringelson  
(503) 378-5865

**Banking Operations  
Manager**

Brady Coy  
(503) 378-2457

**Banking Operations  
Coordinator**

Roseanne Ward  
(503) 378-4990

**Merchant Card/U.S. Bank**

Nikki Main  
(503) 378-2409

**Check Fraud/  
Stop Payments**

Nikki Main  
(503) 378-2409

**Check Image Requests**

Sherry Hayter  
(503) 378-2895

**Check Stock Testing**

Brady Coy  
(503) 378-2457

**Fed Wires/ACH Origination**

Shannon Higgins  
(503) 378-5043

**Local Government  
Investment Pool**

Brady Coy  
(503) 378-2457

**Safekeeping/Debt Service**

Sherry Hayter  
(503) 378-2895

**ACH File Issues**

[ach.exception.notify@ost.state.or.us](mailto:ach.exception.notify@ost.state.or.us)

**Online User  
Password Resets**

[ost.banking@ost.state.or.us](mailto:ost.banking@ost.state.or.us)

**Banking Fax**

(503) 373-1179

**Customer Solutions Team**

[customersolutions@ost.state.or.us](mailto:customersolutions@ost.state.or.us)

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, Oregon 97301

[www.oregon.gov/treasury](http://www.oregon.gov/treasury)