October 2025

OREGON STATE TREASURY

Inside the Vault

State Agency Edition

Cybersecurity Awareness Month

October is Cybersecurity Awareness Month, an international initiative that educates everyone about online safety and empowers individuals and businesses to protect their data from cybercrime. Even amidst large-scale data breaches and cyberattacks, Cybersecurity Awareness Month reminds everyone that there are simple, effective ways to keep yourself safer online, protect your personal data, and ultimately help secure our world.

The theme of this year's Cybersecurity Awareness Month is **Building a Cyber Strong America**—highlighting the need to strengthen the country's infrastructure against cyber threats and ensuring resilience and security. It focuses on our nation's critical infrastructure: government entities and small and medium businesses that are vital to protecting the systems and services that sustain us. Much of the nation's critical infrastructure is owned and operated by state, local, tribal, and territorial governments as well as private companies. Additionally, vendors, suppliers, and other parts of the supply chain that support or are connected to critical infrastructure play a critical cybersecurity role.

Cybersecurity Awareness Month focuses on the top four ways to stay safer online:

- **Use strong passwords and a password manager**. Strong passwords are long, random, and unique to each account, and a password manager helps generate and save them.

(Continued on page 2)

Upcoming Holiday

Due to Veterans Day, Treasury, the Federal Reserve, and financial institutions will be closed on Tuesday, November 11. Customer statements and files will not be produced for November 11 due to the closures. In addition, ACH files sent to KeyBank after the last ACH processing window on Monday, November 10, will not be processed by the bank until Wednesday, November 12, and must have an effective date of November 13 or later.

Interest Rates

Average Annualized Yield	
September	4.60%

Interest Rates	
September 1–30	4.60%

(Continued from page 1)

- **Turn on multi-factor authentication (MFA)**. We need more than a password on our most important accounts like those for e-mail, social media, and financials.
- **Recognize and report scams.** Be cautious of unsolicited messages asking for personal information. Avoid sharing sensitive information or credentials with unknown sources. Report phishing attempts and delete the messages.
- **Update your software**. Ensure your software is up to date, and ensure you have the latest security patches and updates on your devices. Enable automatic updates on software or regularly check for updates if automatic updates are not available.

For more information about ways to keep you and your family safer online, visit www.cisa.gov/cybersecurity-awareness-month and www.staysafeonline.org/cybersecurity-awareness-month.

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 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 general cash management services questions, contact Customer Solutions at customer.solutions@ost.state.or.us.

Unauthorized Paper Debit Form Update

Treasury has an updated C.30 Affidavit of Unauthorized Paper Debit form on its Cash Management Forms webpage that agencies can use to notify Treasury of counterfeit, forged, or otherwise unauthorized check debits. The form is a modified version of U.S. Bank's Affidavit of Unauthorized Paper Debit form, and it replaces Treasury's prior C.30 Affidavit of Unauthorized Paper Debit form along with the following:

- C.16 Affidavit of Altered Item
- C.17 Fraud Collection-Claimant Info
- C.18 Affidavit of Forgery
- C.19 Affidavit Claimant's Forged Endorsement
- C.20a Handwriting Exemplar
- C.20b Handwriting Exemplar

If you have questions about Treasury's cash management forms, contact Banking Operations at ost.banking@ost.state.or.us.

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Bryan Cruz González
503.378.3496

Policy Analyst
Ken Tennies
503.373.7453

Administrative Specialist
Kari McCaw
503.378.4633

▲ ▲ ▲

Customer Solutions Team
customer.solutions@ost.state.or.us
503.373.7312

Analysts
Lyndsie DeOlus
Heidi Lancaster
Ellis Williams

Banking Operations
ACH & Wire Transfers
ost.eft@ost.state.or.us

Banking Services
ost.banking@ost.state.or.us

Fax
infax.ost@ost.state.or.us
503.373.1179

Banking Operations Manager
Sarah Kingsbury
503.373.1501

Banking Operations Coordinator
Jeremiah McClintock
503.378.4990

Bank Analysts
Nikki Main
503.378.2409

Shannon Higgins
503.378.5043

ACH Coordinator
Ashley Moya
503.373.1944

Administrative Accountant
Sherry Hayter
503.378.2895

Banking Support Specialists
Rebecca Jordan
503.566.9432

Jessica Kiefer-Layman
503.373.1234

Cash Management Improvement & Renewal Program
cmirp@ost.state.or.us

Manager
Kelsea Bennett
503.378.3048

Cash Management Analyst
Natalya Cudahey
503.378.8256

Senior Business Analyst
Angel Bringelson
503.378.5865

Business Analysts
Cole Johnson
503.378.3359

Eme Wisniewski
503.378.2457

OREGON STATE TREASURY
867 Hawthorne Ave SE ⏩ Salem, OR 97301-5241
oregon.gov/treasury