October 2021

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Cybersecurity Awareness Month

Protecting your customers' cardholder, bank account, or other sensitive information is a continuous, ongoing process—not a single step or action. Recognizing the importance of cybersecurity awareness, the United States Cybersecurity & Infrastructure Security Agency (CISA) and the National Cyber Security Alliance have designated October as Cybersecurity Awareness Month—an annual campaign to raise awareness about cybersecurity. Treasury participates in this essential event by taking the opportunity to remind our customers of the importance of information security.

Now in its 18th year, the campaign 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 organizations to ensure that 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 Cybersecurity Awareness Month is available at www.cisa.gov/national-cyber-security-awareness-month.

Do Your Part. Be CyberSmart!

Upcoming Holiday

The pool will be closed on Thursday, November 11, for Veterans Day. EON will be available but the system will not allow transactions to settle on the holiday.

Interest Rates

Average Annualized Yield	
September	0.55%

Interest Rates	
September 1–30	0.55%

Stop.Think.Connect

CISA 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 e-mail, 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.
- **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. A password manager can be a helpful tool to keep your passwords long and strong.
- **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 e-mail 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 Stop.Think.Connect campaign at www.cisa.gov/stopthinkconnect.

Tips for keeping your personal information safe, your family protected, and our national security intact.

Stop hackers from accessing your accounts — set secure passwords.
Stop sharing too much information — keep your personal information personal.
Stop — trust your gut. If something doesn't feel right, *stop what you are doing.*

Think about the information you want to share before you share it.
Think how your online actions can affect your offline life.
Think before you act — don't automatically click on links.

Connect over secure networks.
Connect with people you know.
Connect with care and be on the lookout for potential threats.

STOP | THINK | CONNECT™

Securing one citizen, one family, one Nation against cyber threats.

Spear Phishing

All organizations must be vigilant in combatting ever-sophisticated cybercriminals. Spear phishing, in which cybercriminals use target-specific approaches and social engineering, is a particularly challenging scam that often circumvents traditional technological defenses such as spam filters.

While spear phishing attacks can come in many forms, payment instruction switch is a common scam based on a legitimate customer or vendor relationship. In this type of attack, an organization has been regularly paying a customer or vendor via direct deposit. The organization then receives a form, fax, or e-mail updating the customer's or vendor's bank account information used to process payments. In actuality, the update was submitted by a cybercriminal. If undetected, the organization starts sending payments to the cybercriminal's bank account instead of to the customer's or vendor's bank account. Without proper controls and prevention strategies, the organization may lose multiple payments until the customer or vendor notifies the organization of the missing payments. Funds lost in these kinds of attacks are often difficult or impossible to recover.

How to Protect Your Organization

While spear phishing is a sophisticated scam that relies on inside information, there are processes that your organization can use to avoid becoming a victim. In the example above, the organization could have uncovered the attempted fraud by calling the customer or vendor at a known phone number in order to confirm the update. When performing such a call-back process, it is important to use a phone number already on file and not one provided with the requested change.

For more tips related to spear phishing and other social engineering attacks, visit the U.S. Computer Emergency Readiness Team's website at www.us-cert.gov/ncas/tips/ST04-014.

HB 2415: Contract Retainage Requirements

House Bill 2415 (2019) amended ORS 279C.570 related to public improvement contracts exceeding $500,000. The amended statute requires that amounts deducted as retainage for such contracts be deposited in an interest-bearing *escrow* account. *Local Government Investment Pool accounts are not escrow accounts and do not satisfy this requirement*. Treasury is not responsible for determining whether funds placed in the pool by a participant are subject to the escrow account requirement in ORS 279C.570. Local government finance staff should work with their procurement/contracting peers to discuss what forms of retainage their organization plans to use and ensure appropriate solutions are in place.

LGIP: Go Green with Electronic Statements

With the use of EON, it is easier than ever to receive and view pool account statements electronically. Follow these simple steps to go paperless and starting receiving electronic statements:

❶ Log in to EON*

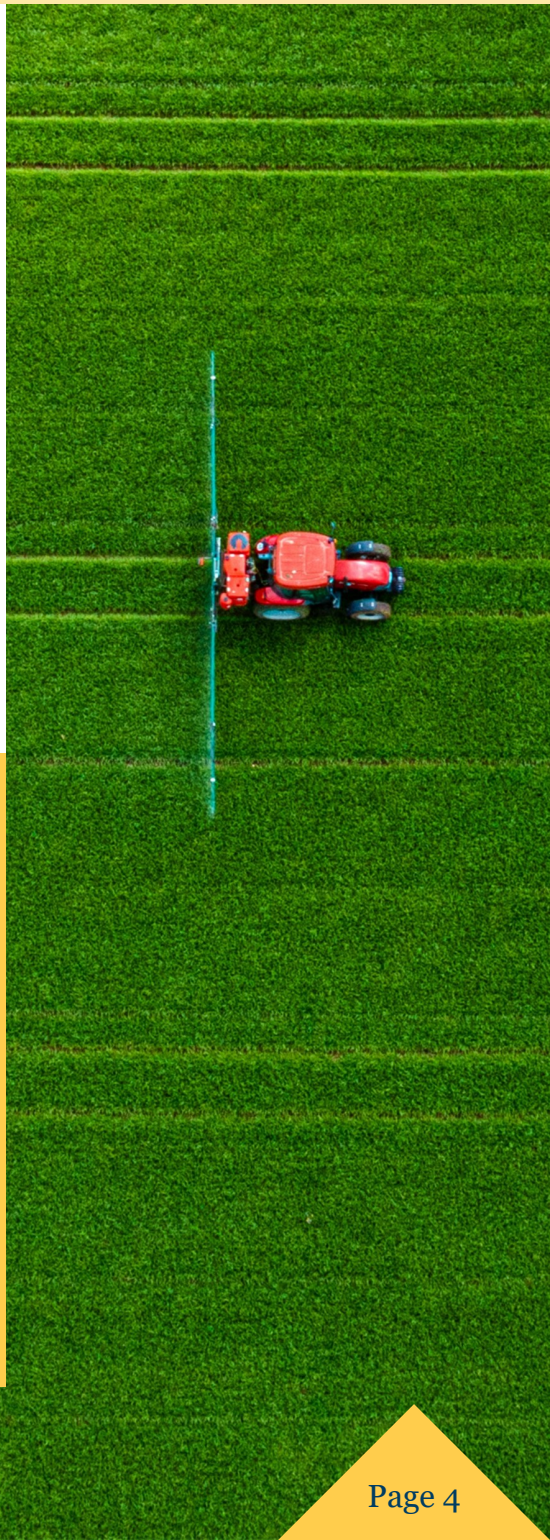
❷ Select Tools/Forms from the top menu

❸ Select Statement Delivery Options

❹ Check the box for "Yes, send me an email notification when my statement is ready to be viewed online" *(optional)*

❺ Click the button Request Electronic Statement Service

**EON access can be established by using an LGIP Contact Registration form with the EON User Information section completed.*



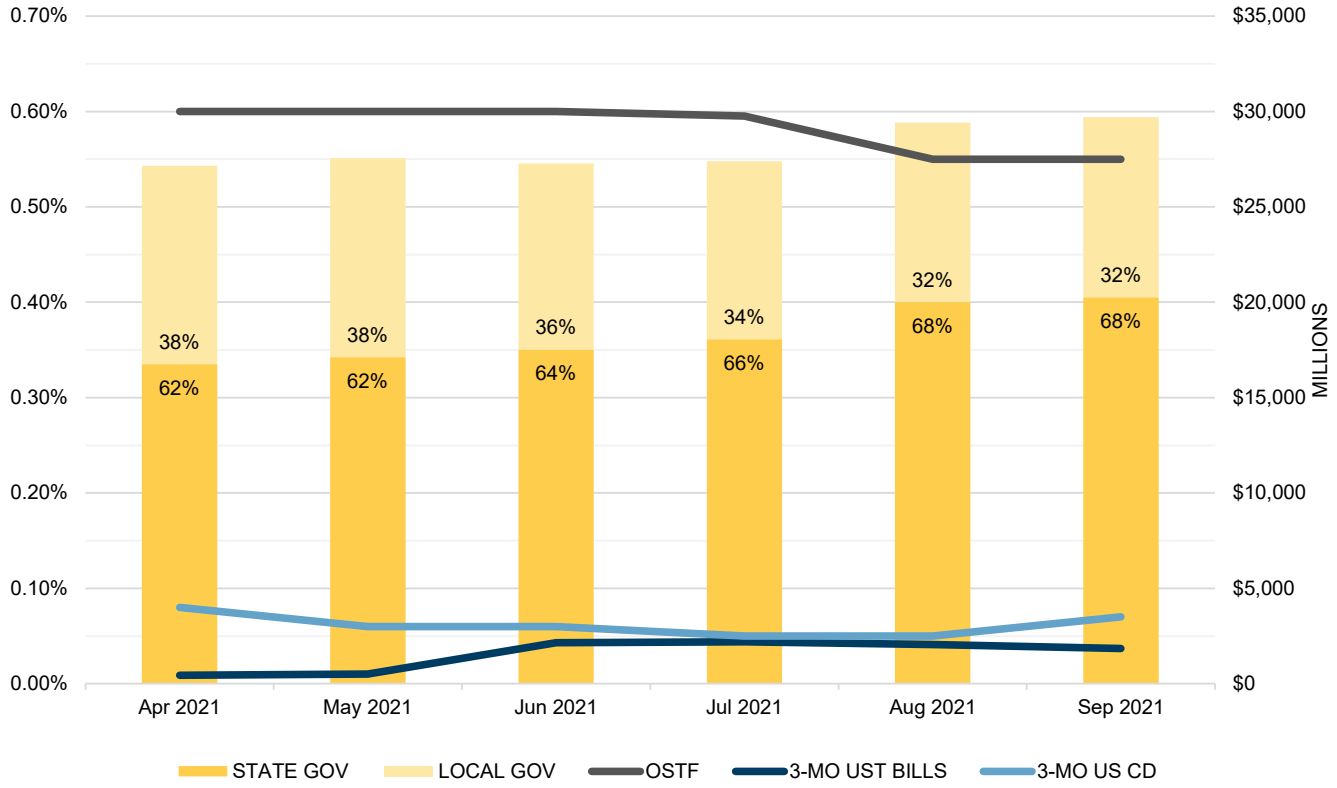
Change to EON Web Address

In preparation for the previously announced purchase of PFM Asset Management by U.S. Bancorp Asset Management, Inc., PFMAM will be changing EON's web address to the new **pfmam.com** domain.

Users will automatically be redirected to the new domain starting Saturday, October 23. Links on Treasury's website will be updated to reflect the new web address, but individual users should update any bookmarks or safe website lists.

If you have any questions about this change or the transaction with USBAM, contact PFMAM Client Services at 800.OST.LGIP or csgwestregion@pfmam.com.

Oregon Short Term Fund Analysis



	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021
TOTAL OSTF AVG DOLLARS INVESTED (MM)	27,154	27,554	27,281	27,393	29,416	29,699
STATE GOV PORTION (MM)	16,749	17,113	17,513	18,065	20,004	20,260
LOCAL GOV PORTION (MM)	10,405	10,441	9,768	9,328	9,412	9,439
OSTF ANNUAL YIELD (ACT/ACT)	0.60	0.60	0.60	0.60	0.55	0.55
3-MO UST BILLS (BOND EQ YLD)	0.009	0.010	0.043	0.044	0.041	0.037
3-MO US CD (ACT/360)*	0.08	0.06	0.06	0.05	0.05	0.07

NOTE: The OSTF ANNUAL YIELD represents the average annualized yield paid to participants during the month. Since interest accrues to accounts on a daily basis and the rate paid changes during the month, this average rate is not the exact rate earned by each account.

3-MO UST BILLS yield is the yield for the Treasury Bill Issue maturing closest to 3 months from month end. 3-MO US CD rates are obtained from Bloomberg and represent a composite of broker dealer quotes on highly rated (A1+/P1/F1+ from Standard & Poor's Ratings Services, Moody's Investors Service and Fitch Ratings respectivley) bank certificates of deposit and are quoted on a CD equivalent yield basis.

Market Data Table

	9/30/2021	1 Month	3 Months	12 Months		9/30/2021	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	0.01	0.01	0.03	0.02	Bloomberg Barclays 1-3 Year Corporate YTW*	0.57	0.50	0.53	0.64
30-Day Agy Nt Disc**	0.01	0.01	0.03	0.03	Bloomberg Barclays 1-3 Year Corporate OAS*	0.32	0.33	0.31	0.58
90-Day Agy Nt Disc**	0.03	0.03	0.03	0.07	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.84	1.83	1.87	1.91
180-Day Agy Nt Disc**	0.05	0.03	0.03	0.08					
360-Day Agy Nt Disc**	0.06	0.02	0.03	0.06	7-Day Muni VRDN Yield**	0.05	0.02	0.03	0.11
					O/N GGC Repo Yield**	0.05	0.06	0.06	0.12
30-Day Treasury Bill**	0.05	0.02	0.03	0.07					
60-Day Treasury Bill**	0.02	0.03	0.03	0.07	Secured Overnight Funding Rate (SOFR)**	0.05	0.05	0.05	0.08
90-Day Treasury Bill**	0.02	0.03	0.03	0.08					
6-Month Treasury Yield**	0.05	0.05	0.05	0.10	US 10 Year Inflation Break-Even**	2.38	2.34	2.34	1.63
1-Year Treasury Yield**	0.07	0.07	0.07	0.12					
2-Year Treasury Yield**	0.28	0.21	0.25	0.13	1-Day CP (A1/P1)**	0.09	0.14	0.16	0.08
3-Year Treasury Yield**	0.51	0.41	0.46	0.16	7-Day CP (A1/P1)**	0.09	0.12	0.15	0.06
					30-Day CP (A1/P1)**	0.10	0.09	0.12	0.11
1-Month LIBOR**	0.08	0.08	0.10	0.15					
3-Month LIBOR**	0.13	0.12	0.15	0.23	30-Day CD (A1/P1)**	0.07	0.08	0.07	0.14
6-Month LIBOR**	0.16	0.15	0.16	0.26	90-Day CD (A1/P1)**	0.10	0.11	0.10	0.18
12-Month LIBOR**	0.24	0.23	0.25	0.36	6-Month CD (A1/P1)**	0.16	0.15	0.14	0.25
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	0.21	0.21	0.20	0.36

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Mike Auman
503.378.2752

Newsletter Questions
Kari McCaw
503.378.4633

Bryan Cruz González
503.378.3496

Local-Gov-News Mailing List
omls.oregon.gov/mailman/listinfo/local-gov-news

Local Government Investment Pool
oregon.gov/lgip

PFM Client Services
855.OST.LGIP
csgwestregion@pfmam.com

- EON Access
- Transactions
- Reporting
- Account/User Maintenance
- Eligibility

Treasury
800.452.0345
lgip@ost.state.or.us

- Investment Management
- Statutory Requirements
- Service Provider Issues
- General Program Inquiries

Oregon Short Term Fund Staff
503.431.7900

Public Funds Collateralization Program
oregon.gov/pfcp
503.378.3400
public.funds@ost.state.or.us

OREGON STATE TREASURY
350 Winter Street NE, Suite 100 ›› Salem, OR 97301-3896
oregon.gov/treasury