OREGON STATE TREASURY

Inside the Vault

Local Government Edition

National Cybersecurity Awareness Month

The first three months of 2020 saw a 20% increase in cyber fraud as cybercriminals took advantage of the global pandemic.

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 Cybersecurity & Infrastructure Security Agency (CISA) and the National Cyber Security Alliance have 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.

2020 marks the 17th 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 www.cisa.gov/national-cyber-security-awareness-month.

Upcoming Holiday

The pool will be closed on Wednesday, 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	1.00%

Interest Rates	
September 1–30	1.00%

LGIP Investor Webinar Series

The pandemic continues to affect how we all live and work. And while we need to keep our distance during these challenging times, it's also important that we stay connected.

To stay connected with you, our customers, this year's LGIP Investor Meeting will be held as a series of webinars. This free event—spread across four days—will provide an opportunity to learn more about the pool, the outlook for financial markets, and other public finance topics.

Sessions will run Monday, November 16 through Thursday, November 19. And because flexibility is key right now, you can join the webinars at the scheduled times or catch up with recordings afterward.

Treasury is proud to be your financial partner and we understand that now, more than ever, you're relying on us to safeguard public funds and to lead the way toward long-term financial security.

Visit our website for a full list of webinar sessions and to meet our presenters, or reserve your spot now by registering online. We hope you're able to join us for this valuable event.

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:

1. Log in to EON*
2. Select Tools/Forms from the top menu
3. Select Statement Delivery Options
4. Check the box for "Yes, send me an email notification when my statement is ready to be viewed online" *(optional)*
5. 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.*

Spear Phishing

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, 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.

Staff Update

Angela Schaffers will soon transition within Treasury to a new role with the Private Equity team. For the past five and a half years, Angela has helped the Fixed Income team manage the Oregon Short Term Fund (OSTF) as an investment analyst. As part of that team, she has played an integral role in daily fund management and contributed to the fund's consistently strong investment performance. Angela is well known for her strong relationships with Treasury's customers and as the driving force behind the successful LGIP Investor Meeting. We greatly appreciate Angela's work with the OSTF and are glad that her talents and dedication will continue to serve Treasury and our customers as she joins the Private Equity team.

Management of the OSTF remains piloted by the experienced, capable hands of the Fixed Income team, who include Perrin Lim, Will Hampson, John Lutkehaus, and Geoff Nolan. Until Angela's replacement is identified, do not hesitate to contact Perrin at perrin.lim@ost.state.or.us, Jeremy Knowles at jeremy.knowles@ost.state.or.us, or other members of the team at 503.431.7900 with investment –related questions. Thank you for your continued investment in and support of the OSTF.

Reminder: EON Security Enhancements

Treasury is continuously focused on protecting public funds and our customers' financial data. As part of these efforts, and in recognition of October being National Cybersecurity Awareness Month, we are excited to announce three EON security enhancements that will start rolling out on Wednesday, October 28.

Multi-Factor Authentication

Multi-factor authentication (MFA) is an industry leading practice for verifying a user's identity. Once enabled, EON users will be prompted to enter a one-time numeric passcode immediately after entering your user name and password. Users can choose to receive the passcode by e-mail, phone call, or text message. Once you have selected the delivery method, you will receive the passcode and then enter it in EON to complete your login. To prepare for MFA, log in to EON today and verify your contact information by clicking on "Profile Update" at the top of the page.

Account Activity Notification Center

The account activity notification center is a communication tool that will provide additional insight into account activity and help mitigate fraud. EON users will receive e-mail notifications of key account activities—including certain transactions and changes to both ACH/wire instructions and user permissions—based on individual account permissions and subscription preferences.

Increased Password Complexity

Newly increased password complexity requirements will mean that EON users must use passwords that meet current industry best practices. If a user's existing password does not meet the new requirements, the user will be prompted to create a new password when logging in. As the user types the new password, EON will list the requirements and indicate which are met or unmet. A user's new password must meet all requirements before EON will accept the new password.

More information about these security enhancements is available within EON under "Reports > EON Enhancements," and we hope you join Treasury in recognizing the value of these security enhancements.

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 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.
- **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 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.*

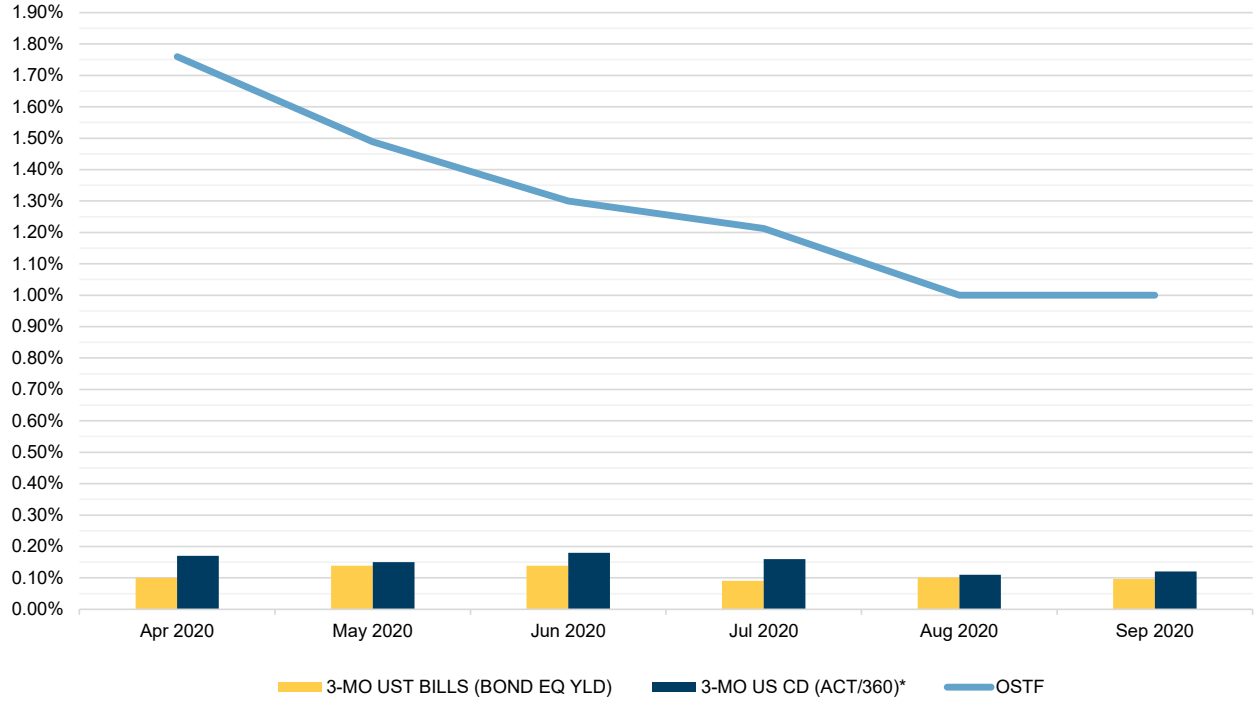
Think about the information you want to share before you share it.
Think how your online actions can affect your offline life.
Think before you act — don't automatically click on links.

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.

Oregon Short Term Fund Analysis



	Apr 2020	May 2020	Jun 2020	Jul 2020	Aug 2020	Sep 2020
TOTAL OSTF AVG DOLLARS INVESTED (MM)	22,717	23,839	22,921	22,909	23,591	23,016
STATE GOV PORTION (MM)	13,153	14,420	14,307	14,583	15,019	14,519
LOCAL GOV PORTION (MM)	9,564	9,419	8,614	8,326	8,572	8,497
OSTF ANNUAL YIELD (ACT/ACT)	1.76	1.49	1.30	1.21	1.00	1.00
3-MO UST BILLS (BOND EQ YLD)	0.100	0.139	0.139	0.091	0.101	0.097
3-MO US CD (ACT/360)*	0.17	0.15	0.18	0.16	0.11	0.12

NOTE: The OST ANNUAL YIELD represents the average annualized yield paid to account holders 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.

This material is available in alternative format and media upon request.

Market Data Table

	9/30/2020	1 Month	3 Months	12 Months		9/30/2020	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	0.02	0.07	0.03	1.74	Bloomberg Barclays 1-3 Year Corporate YTW*	0.64	0.59	0.80	2.11
30-Day Agy Nt Disc**	0.03	0.08	0.09	1.80	Bloomberg Barclays 1-3 Year Corporate OAS*	0.58	0.52	0.73	0.50
90-Day Agy Nt Disc**	0.07	0.08	0.12	1.83	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.91	1.89	1.92	1.85
180-Day Agy Nt Disc**	0.08	0.08	0.13	1.79					
360-Day Agy Nt Disc**	0.06	0.08	0.14	1.78	7-Day Muni VRDN Yield**	0.11	0.09	0.13	1.58
					O/N GGC Repo Yield**	0.12	0.12	0.13	1.83
30-Day Treasury Bill**	0.07	0.07	0.10	1.75					
60-Day Treasury Bill**	0.07	0.08	0.11	1.73	Secured Overnight Funding Rate (SOFR)**	0.08	0.09	0.10	2.35
90-Day Treasury Bill**	0.08	0.08	0.12	1.75					
6-Month Treasury Yield**	0.10	0.11	0.16	1.82	US 10 Year Inflation Break-Even**	1.63	1.80	1.34	1.52
1-Year Treasury Yield**	0.12	0.12	0.15	1.76					
2-Year Treasury Yield**	0.13	0.13	0.15	1.62	1-Day CP (A1/P1)**	0.08	0.07	0.08	1.90
3-Year Treasury Yield**	0.16	0.15	0.17	1.56	7-Day CP (A1/P1)**	0.06	0.10	0.11	1.92
					30-Day CP (A1/P1)**	0.11	0.12	0.15	1.97
1-Month LIBOR**	0.15	0.16	0.16	2.02					
3-Month LIBOR**	0.23	0.24	0.30	2.09	30-Day CD (A1/P1)**	0.14	0.12	0.20	2.02
6-Month LIBOR**	0.26	0.31	0.37	2.06	90-Day CD (A1/P1)**	0.18	0.19	0.29	2.08
12-Month LIBOR**	0.36	0.45	0.55	2.03	6-Month CD (A1/P1)**	0.25	0.26	0.41	2.08
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	0.36	0.31	0.56	1.99

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
cswestregion@pfm.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

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