November 2022

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Scholarship for Underrepresented and Diverse Students

The Oregon College Savings Plan has opened this year's application for its *Diversity in Leadership Scholarship*. The scholarship supports underrepresented and diverse Oregon high school graduates pursuing higher education in the state. Awards may be used to attend a range of Oregon institutions, including apprenticeships, trade schools, community colleges, colleges, or universities. *Applications are due by Wednesday, March 1, 2023, for the following academic year.*

The scholarship is administered through the Oregon Community Foundation's scholarship program. Two recipients are selected each year, with awardees receiving $10,000 for their freshman year and $5,000 for each of the next three years of full-time enrollment, or until completion of degree (whichever comes earlier).

"This scholarship is an investment, aimed at making Oregon's future more inclusive, and we're gratified to support the education journeys of promising students," said State Treasurer Tobias Read.

To apply for the scholarship or to find more information, visit www.oregoncollegesavings.com/diversity-in-leadership-scholarship.

Upcoming Holiday

The pool will be closed on Thursday, November 24, for Thanksgiving. Connect will be available but the system will not allow transactions to settle on the holiday.

Interest Rates

Average Annualized Yield

October	2.1032%

Interest Rates

October 1–10	1.90%
October 11–31	2.20%

Security Spotlight: Social Engineering

It is the end of a long day and you finally get around to checking the voicemail left by an unknown number that called earlier. A voice informs you that you owe back taxes to the IRS and there is a warrant out for your arrest, so please call back. Did you remember to mail your local taxes? Did your mortgage company make that payment? Maybe it is someone with the same name? It has to be a mistake, but you need to know for sure. Do you call the number?

What Is Social Engineering?

Social engineering is the art of capitalizing on relationships and social behavior to manipulate people into providing access, supplying information, or performing an action. An attack can be as simple as an unsolicited e-mail that appears to be from a friend pleading for help or as elaborate as a request from your supervisor directing you to perform an action immediately. In every case, people are the key to whether an attack succeeds or fails.

What Are Some Different Types of Social Engineering?

Attacks are usually distinguished by the medium used or the type of pressure exerted on a victim. One of the most common examples are "phishing attacks." These e-mails look like legitimate requests and usually come with a degree of urgency to get a victim to act quickly. If a recipient accepts the e-mail as legitimate, they may click a link, provide confidential information, and continue about their business unaware that sensitive information is now in the hands of hackers. The access provided can allow hackers to lurk in a system, exploiting any information available to achieve their ultimate goal.

A simple phishing attack can be just the beginning. The more information hackers have about an individual or organization, the more they are able to make their attacks convincing, potentially leading to "spear phishing." Spear phishing is when hackers understand the relationships within an organization and send e-mails designed to mimic requests within the organization. Many people refuse to click on links in a strange e-mail, but suppose it is an urgent request from supervisor? Many recipients are less likely to verify if the request is legitimate or an attack before reacting.

Attacks are not limited to e-mail communication or a specific tactic. Any mode of communication or predictable tendency can be exploited. Here is a list of some of the other common attacks:

- **Vishing** (voice-phishing) attacks are the same as both phishing and spear phishing attacks, but are done through telephone calls
- **Smishing** (SMS-phishing) attacks utilize text messages
- **Pretexting** presents victims with the false "pretext" of verifying their information
- **Baiting** offers victims a prize for information
- **Tailgating** takes advantage of holding a door open to compromise a secure location
- **Quid Pro Quo** attacks give victims a gift to make them feel obligated to respond

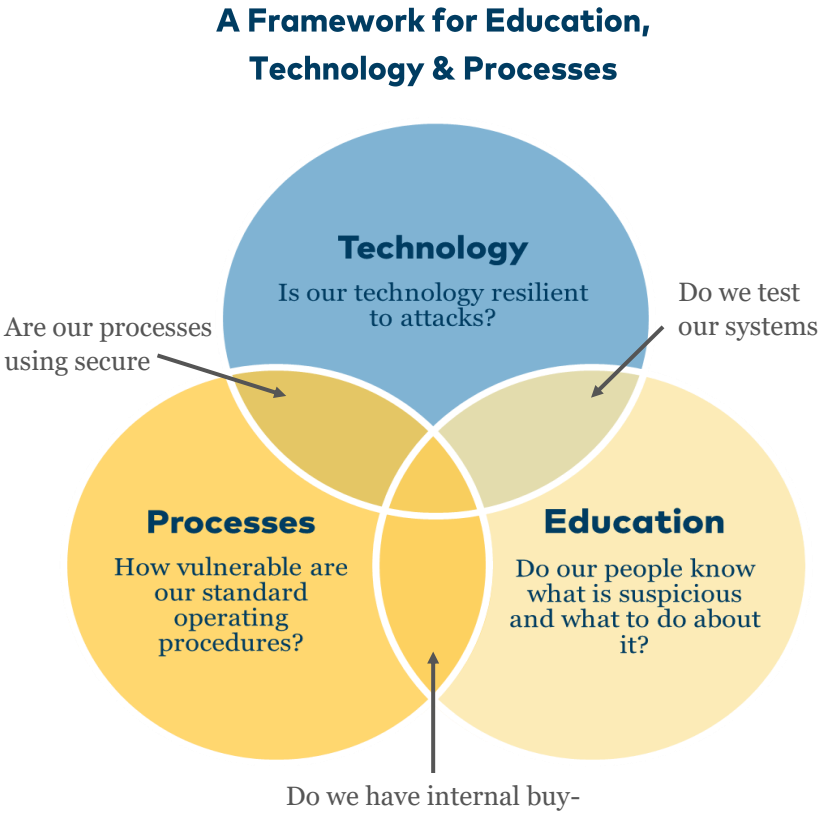
(Continued on page 3)

(Continued from page 2)

Ultimately, hackers employ these methods because they are much easier than trying to hack into software. Every software system is designed to be used by users, so the surest way to gain control is to manipulate the user.

How Can I Help Protect against Social Engineering Attacks?

We encourage all of our customers to think about their readiness, specifically how your organization can prepare by deploying technology, processes, and education designed to enhance security.



Attacks are a product of technology, but technology can also play a role in protection. For instance, spam filters are effective at stopping most phishing e-mails from reaching intended targets. Another tool is multi-factor authentication (MFA). MFA is a method of confirming a user's identity utilizing factors beyond the standard username and password. Sometimes simple procedures like regularly resetting passwords can limit damage or frustrate attacks.

Unfortunately, deploying more secure technology in an organization does not mean it gets used every time, a fact that highlights the importance of assessing organizational processes. Process assessment should extend to third-party service providers as well, and be understood by all parties.

Finally, education should underpin any readiness effort. Any person with even low levels of access to data should have a basic knowledge of what attacks are possible through e-mail, text, and phone. Employees of public organizations face a unique challenge in that they are responsible for providing transparency but any information—such as organizational charts, contact information, and biographical information—could be used to hijack internal communications. Educational efforts should highlight what is possible and underscore the security reasons behind the processes and technology that employees execute or interact with on a daily basis.

So Do You Call Them Back?

We hope that after understanding the possibilities that technology has opened for both good and malicious purposes, you know that the best course of action is to delete the voicemail mentioned in the opening scenario. If you wanted to go the extra step, you could contact the IRS directly, being careful not to use any contact information from the message. Although these attacks can be alarming, hackers using social engineering have no way to keep you from simply deleting an e-mail or independently verifying any suspicious requests.

LGIP Redemptions: Wire Transfer vs. ACH

Participants have two options when redeeming (withdrawing) funds. Understanding the differences between wire transfer and ACH will help you best meet your business needs.

Wire Transfer	ACH
Can settle as soon as same day (must be initiated by 10:00 a.m.)	Can settle as soon as next business day (must be initiated by 1:00 p.m.)
Same-day wire transfers cannot exceed $1.5 million (no dollar limit for future-dated wire transfers)	No dollar limit
$10.00 fee per transaction	$0.05 fee per transaction

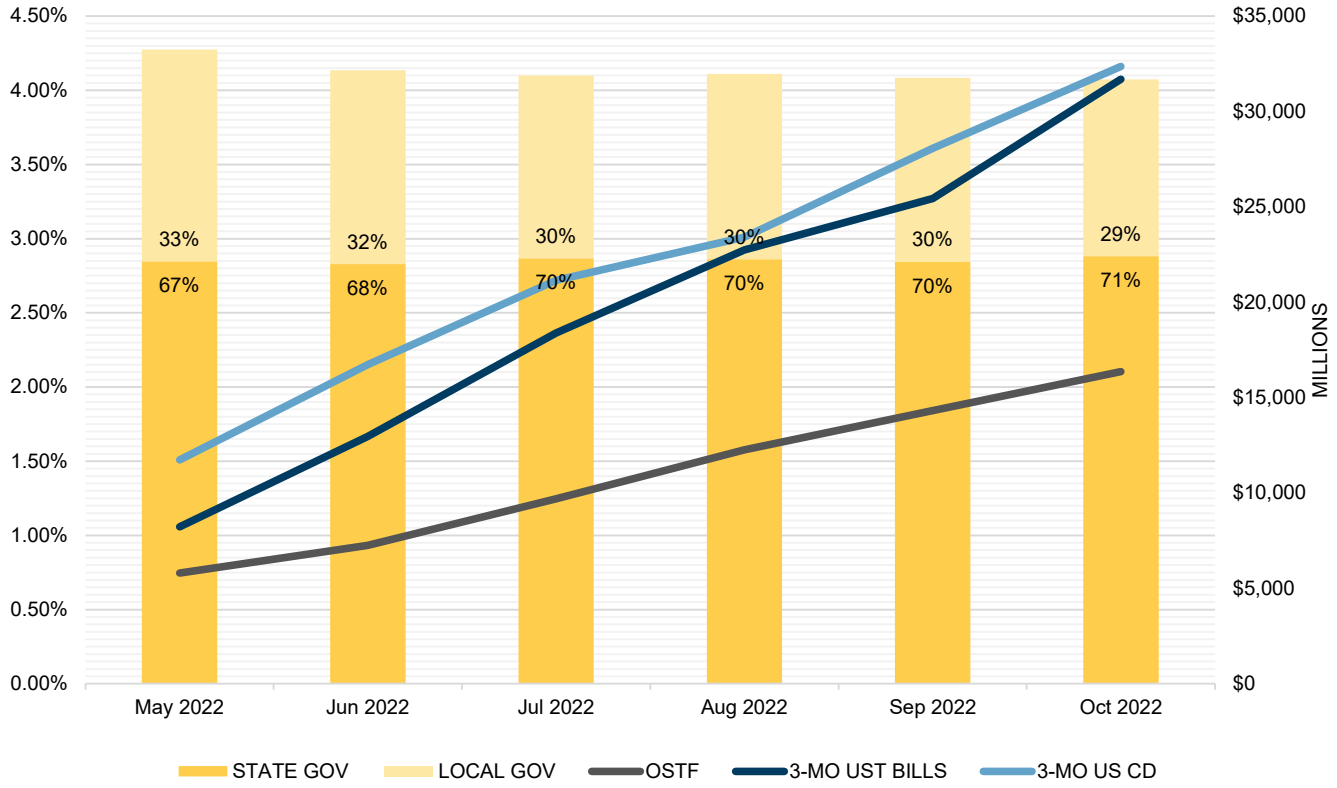
If you need to redeem funds immediately, wire transfer is the only option available (note that same-day wire redemptions cannot exceed $1.5 million). If you do not need funds the same day, ACH may be the best option given its lower cost. Both types of transactions can be scheduled up to almost a year in advance. Contact PFMAM Client Services at 855.OST.LGIP or csgwestregion@pfmam.com if you have questions about which redemption option best meets your needs.

2023 LGIP Holiday Schedule

The Local Government Investment Pool will be closed on the following holidays throughout 2023. EON will be available but the system will not allow transactions to settle on a holiday.

Day	Date	Holiday
Monday	January 2	New Year's Day (observed)
Monday	January 16	Martin Luther King, Jr. Day
Monday	February 20	Presidents Day
Monday	May 29	Memorial Day
Monday	June 19	Juneteenth
Monday	July 4	Independence Day
Monday	September 4	Labor Day
Monday	October 9	Columbus Day
Thursday	November 23	Thanksgiving
Monday	December 25	Christmas

Oregon Short Term Fund Analysis



	May 2022	Jun 2022	Jul 2022	Aug 2022	Sep 2022	Oct 2022
TOTAL OSTF AVG DOLLARS INVESTED (MM)	33,245	32,158	31,884	31,978	31,769	31,678
STATE GOV PORTION (MM)	22,145	21,998	22,297	22,255	22,114	22,414
LOCAL GOV PORTION (MM)	11,100	10,160	9,587	9,723	9,655	9,264
OSTF ANNUAL YIELD (ACT/ACT)	0.75	0.93	1.25	1.58	1.84	2.10
3-MO UST BILLS (BOND EQ YLD)	1.058	1.667	2.364	2.925	3.270	4.074
3-MO US CD (ACT/360)*	1.51	2.15	2.72	3.01	3.61	4.16

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

	10/31/2022	1 Month	3 Months	12 Months		10/31/2022	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	2.84	2.85	1.81	0.04	Bloomberg Barclays 1-3 Year Corporate YTW*	5.43	5.08	3.61	0.80
30-Day Agy Nt Disc**	3.54	3.02	2.16	0.04	Bloomberg Barclays 1-3 Year Corporate OAS*	1.01	0.88	0.80	0.39
90-Day Agy Nt Disc**	3.95	3.44	2.52	0.04	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.90	1.92	1.95	1.84
180-Day Agy Nt Disc**	4.40	3.93	2.89	0.04					
360-Day Agy Nt Disc**	3.79	3.86	2.74	0.09	7-Day Muni VRDN Yield**	2.24	2.46	1.33	0.05
					O/N GGC Repo Yield**	3.05	3.00	2.32	0.02
30-Day Treasury Bill**	3.44	2.60	2.09	0.04					
60-Day Treasury Bill**	3.70	2.90	2.17	0.05	Secured Overnight Funding Rate (SOFR)**	3.05	2.98	2.27	0.05
90-Day Treasury Bill**	3.96	3.20	2.36	0.05					
6-Month Treasury Yield**	4.54	3.93	2.86	0.06	US 10 Year Inflation Break-Even**	2.51	2.15	2.55	2.59
1-Year Treasury Yield**	4.64	3.99	2.94	0.12					
2-Year Treasury Yield**	4.49	4.28	2.89	0.50	1-Day CP (A1/P1)**	3.18	3.01	1.54	0.04
3-Year Treasury Yield**	4.44	4.29	2.81	0.76	7-Day CP (A1/P1)**	3.28	2.99	2.30	0.06
					30-Day CP (A1/P1)**	3.64	3.10	2.35	0.07
1-Month LIBOR**	3.80	3.14	2.36	0.09					
3-Month LIBOR**	4.46	3.75	2.79	0.13	30-Day CD (A1/P1)**	3.85	3.38	2.33	0.11
6-Month LIBOR**	4.92	4.23	3.33	0.20	90-Day CD (A1/P1)**	4.50	3.63	2.73	0.16
12-Month LIBOR**	5.45	4.78	3.71	0.36	6-Month CD (A1/P1)**	4.93	4.23	3.32	0.20
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	6.37	4.73	2.95	0.33

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Bryan Cruz González
503.378.3496

Newsletter Questions
Kari McCaw
503.378.4633

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

Local Government Investment Pool
oregon.gov/lgip

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

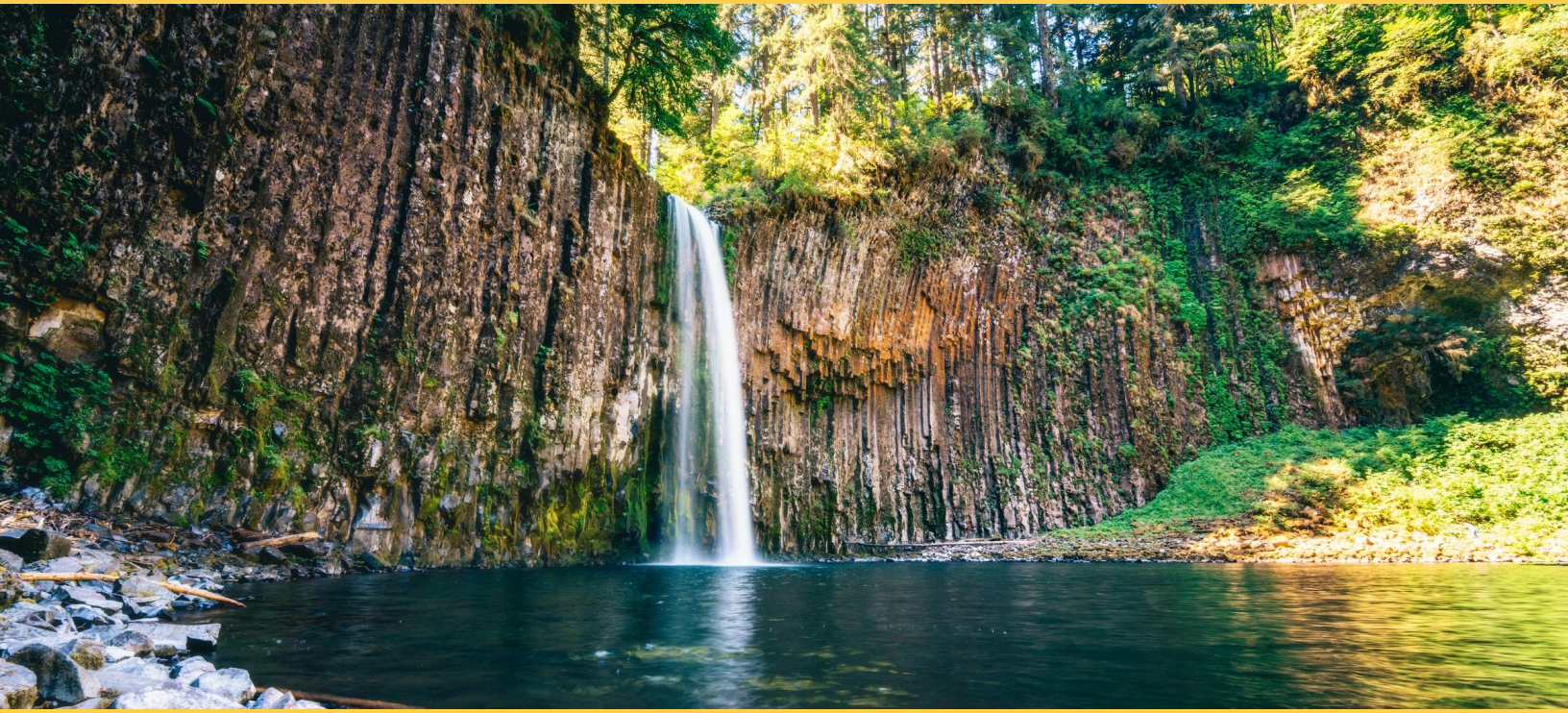
- Connect Access
- Transactions
- Reporting
- Account/User Maintenance
- Eligibility

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