February/March 2023

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Public Funds Reminder

All public funds in Oregon must be deposited in compliance with the requirements of ORS chapter 295. Public officials may deposit public funds up to the amount insured by the Federal Deposit Insurance Corporation (FDIC) or National Credit Union Administration (NCUA) —currently $250,000—in any insured financial institution with a head office or branch located in Oregon. Public funds balances that exceed those insurance limits, however, must be held at a depository qualified under Treasury's Public Funds Collateralization Program (PFCP).

Through the PFCP, depositories pledge collateral to secure any public funds deposits that exceed insurance amounts, providing additional protection for public funds in the event of a depository loss or failure. ORS chapter 295 specifies the value of the collateral—as well as the types of collateral that are acceptable—and creates a shared liability structure for participating depositories, minimizing (though not eliminating) the risk of loss of such funds.

OAR 170-040-0050 requires public entities to annually verify their contact information as well as the list of all banks and credit unions where the entities' funds are deposited. Treasury recently sent out verification requests to entities that have previously provided this information. *A response to Treasury's request is required by the included due date to remain in compliance with state law.*

Additional information regarding PFCP can be found at www.oregon.gov/pfcp.

For further information, contact PFCP staff at 503.378.3400 or public.funds@ost.state.or.us.

Interest Rates

Average Annualized Yield	
January	3.3742%
February	3.7500%

Interest Rates	
Jan. 1–5	3.10%
Jan. 6–26	3.35%
Jan. 27—Feb. 28	3.75%

Security Spotlight: Phishing

Now that many organizations have employees splitting time working in the office and remotely, cybercriminals are using phishing attempts that exploit a lack of close coordination with coworkers or business contacts. Other common phishing attempts include the following:

- **Account Locked or Disabled E-mails.** Recipients receive e-mails that indicate an account from a site like Amazon, Apple, or Microsoft is locked or disabled. These e-mails ask the recipient to click a link and enter their credentials. The link directs users to a fake site where it captures login information.
- **News and "Clickbait" Pieces.** Many people are hungry for news concerning current events. There are a plethora of fake news and clickbait sites that include articles that contain what may seem like outlandish news, simply to spur users to click a link. The site then may install a virus or other malware.
- **Charitable Donations or Prize E-mails.** Scammers frequently seek to prey on emotions. They may circulate sob stories to solicit donations to fake charities or may promise that a user has won money, a gift card, or a free vacation. These attempts can capture banking information, either under the guise of a donation or require this information in order to provide a prize.
- **Coworker Needs Help E-mail.** One may receive a spoofed e-mail that appears to be from a coworker asking for assistance, often adding a sense of urgency.

How to Avoid Falling Prey to a Phishing Attempt

There are many ways one can avoid taking the phishing bait. The best way to prevent phishing attacks is through training concerning cybersecurity. Other steps you can take include:

- If you receive an "account locked" e-mail, do not click the link. Instead, go directly to the site and determine if the account is really locked. If it is locked, use only the links on the site to reset a password.
- Visit only well-known and recognized news and information sites. If a URL appears similar but has additional letters or numbers, go to the main site and search for the information there.
- Do not donate to charities via an e-mail link. Go directly to the charity's website and donate via their webpage. If you do not remember entering a contest and can find no record of it on the organization's website, you likely are being scammed. Use common sense and skepticism.
- When an odd e-mail from a coworker is received, or an e-mail requesting money or assistance with something that normally would not be handled via e-mail, reach out to the contact via phone, or by sending a separate e-mail to that contact. Do not reply to the initial e-mail and do not take the steps requested in the e-mail without first confirming it is legitimate.
- Never open attachments from unknown sources or unexpected e-mails. Confirm with the sender via phone or direct e-mail they sent information via an attachment.

We live in a complex world where cybercriminals seek to capitalize on current events as much as possible. Employees must be aware of this and must always be vigilant to help protect organizations from cyberattacks.

LGIP: Your Customer Support Team

PFMAM Client Services is available by phone to answer questions, perform account maintenance, and process transactions. Support is available from 7:00 a.m. to 4:00 p.m. Pacific, Monday through Friday, at 855.OST.LGIP.

Jeremy King is a Key Account Manager in PFMAM's Client Services Group. Jeremy serves as a client advocate providing a "high-touch, high-value" experience, whatever the client's additional needs may be. Additionally, his responsibilities are to coordinate the efforts of the customer service team in everyday functions. These functions include interacting daily with Oregon participants, serving their needs, answering any questions they may have, on-boarding new relationships, maintaining existing relationships, and client administration. Jeremy graduated from Pennsylvania State University, and he spends his free time at the beach, enjoys kayaking, and is involved in pet rescue and fostering.

Rachael Miller is a Client Consultant in PFMAM's Client Services Group. Rachael focuses on providing superior client service by answering client requests regarding account activity, updating personnel and account specific information, and training new colleagues. She has formed and maintained positive relationships with clients, making their experience working with PFMAM a positive one. Rachael is a graduate of Millersville University and enjoys spending time with her family and friends, running, cooking, and traveling.

DeWayne Fields is a Client Service Representative in PFMAM's Client Services Group. DeWayne is committed to providing exceptional client service through clear communication, accuracy, and understanding. By creating and maintaining effective relationships with clients, he can recognize and assist customer needs, answer questions in a timely manner, and provide proactive follow up.

Contract Retainage Requirements

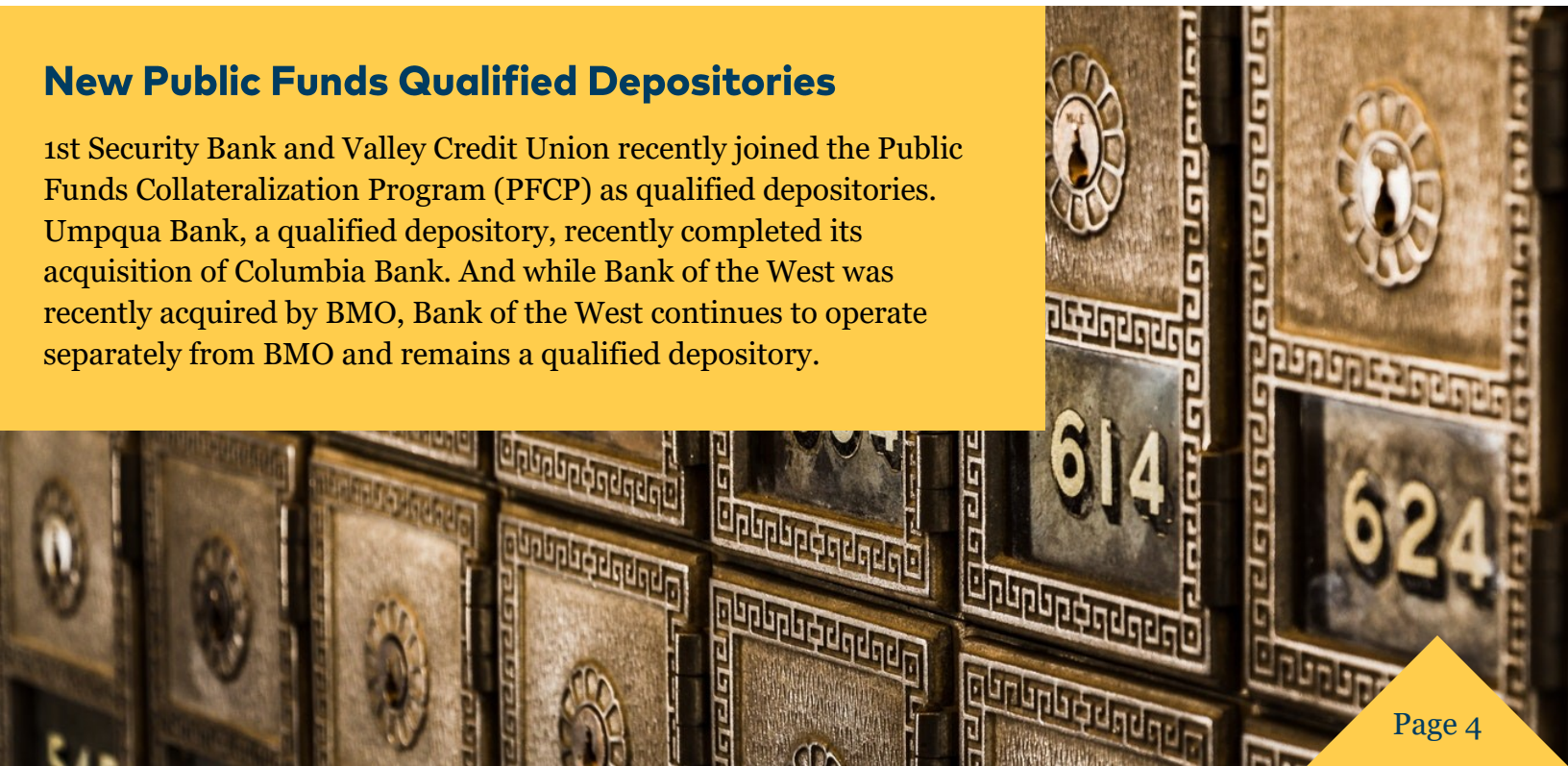
House Bill 2415 (2019) amended ORS 279C.570 related to public improvement contracts exceeding $500,000. The amended statute requires that amounts deducted as cash retainage for such contracts be deposited in an interest-bearing escrow account unless a contractor requests an alternate approach (current House Bill 2870 would remove the escrow requirement). 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.

Public Funds Qualified Depositories

- 1st Security Bank
- Advantis Credit Union
- Baker Boyer Bank
- Bank of America
- Bank of Eastern Oregon
- Bank of the Pacific
- Bank of the West
- Banner Bank
- Beneficial State Bank
- Central Willamette Credit Union
- Chase Bank
- Citizens Bank
- Clackamas County Bank
- Commerce Bank of Oregon
- Community Bank
- First Community Credit Union
- First Federal
- First Interstate Bank
- Heritage Bank
- HomeStreet Bank
- InRoads Credit Union
- KeyBank
- Lewis & Clark Bank
- Maps Credit Union
- Northwest Bank
- Northwest Community Credit Union
- Old West Federal Credit Union
- OnPoint Community Credit Union
- Oregon Coast Bank
- Oregon Community Credit Union
- Oregon Pacific Bank
- Oregon State Credit Union
- Pacific Crest Federal Credit Union
- Pacific West Bank
- People's Bank
- Riverview Community Bank
- Rogue Credit Union
- Summit Bank
- Umpqua Bank
- Union Bank
- Unitus Community Credit Union
- U.S. Bank
- Valley Credit Union
- WaFd Bank
- Washington Trust Bank
- Wauna Credit Union
- Wells Fargo Bank

New Public Funds Qualified Depositories

1st Security Bank and Valley Credit Union recently joined the Public Funds Collateralization Program (PFCP) as qualified depositories. Umpqua Bank, a qualified depository, recently completed its acquisition of Columbia Bank. And while Bank of the West was recently acquired by BMO, Bank of the West continues to operate separately from BMO and remains a qualified depository.



Security Spotlight: Data Breaches

More than a decade ago, a data breach forced many organizations to realize the consequences of exposing protected data to unauthorized access and manipulation. Laws were established in response to this first "major" breach, and sensitivity to cyberattacks heightened. Fast forward to today, and that early breach seems practically insignificant compared to the recent Capital One data breach that exposed the personal data of more than 100 million people.

Bringing awareness to how data breaches can occur and the damage they can cause to the clients we serve is part of our turnkey approach to client service. Below, we discuss the current trend of data breaches and how you can be more prepared should a data breach happen to you.

What is a Data Breach?

Unlike cyberattacks such as ransomware, a data breach is the result of a social engineering attack that provides unauthorized access to steal confidential personal or financial data.

Current trends show that cybercriminals steal data for its monetary value, that many companies are not properly prepared for breaches, and that the number of breaches continues to increase each year. What is causing this upward trend?

- **Employee Errors:** The leading cause of data breaches around the world is employee error. These errors come in the form of compromised credentials or lost or stolen devices like company cell phones and laptops. Employee error can be caused by a lack of general awareness for how to handle, retain, and dispose of sensitive data. And a general lack of training can leave employees vulnerable to cybercriminals.
- **Phishing Attacks:** Hackers use social engineering tactics to capitalize on relationships and social behavior to manipulate people into providing access, supplying information, or performing an action. Hackers use emails, texts, or phones calls disguised as legitimate requests to trick employees into unknowingly providing protected information or unauthorized access.

- **Weak or Stolen Credentials:** Phishing attacks are often designed to obtain a user's credentials. In a study of 905 phishing attacks, 91% were found to be targeting usernames and passwords. Password guessing software is also used to search for weak credentials — passwords that are repeatedly used or that contain personal or easily-guessed information.
- **Ransomware:** This is a type of malicious software that infects, locks, or takes control of a system or encrypts important data then demands a ransom to undo it. Ransomware typically falls into two categories:

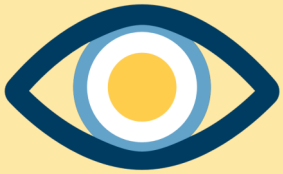
    1. Locker Ransomware - locks a user out of a system but typically leaves the underlying system and files untouched.
    2. Crypto Ransomware - encrypts files stored on a user's computer or mobile device rendering them unreadable until the victim pays for the decryption key.

  Ransomware is typically installed through a malicious email attachment, an infected software download, or a visit to a malicious website. Payment requests are made in hard-to-trace bitcoins, wire services, or

(Continued on page 6)

(Continued from page 5)

gift cards. Paying the ransom does not guarantee the encrypted files will be released. Ransomware has been used against local governments and often prevent the delivery of critical services.



- **Spyware:** This type of attack often occurs when an employee unknowingly downloads spyware thinking they are performing a routine update or running a seemingly nonthreatening computer program. Instead, the malware infects a computer or network and steals personal information or other data.
- **Third-Party Vendors:** As trusted partners for your organization, vendors can sometimes become unsuspecting accomplices to cyberattacks leading to data breaches. A survey by eSentire that interviewed 600 IT professionals determined that nearly half of the respondents experienced a data breach caused by a vendor, that 26% of the breaches were caused by employee errors and stolen passwords, and that the remaining breaches were the result of some form of malware such as spyware.
- **Outdated Software:** Software companies routinely alert users to available updates that provide important software patches to fix identified vulnerabilities. When these updates are overlooked or delayed by employees, it leaves them open to hackers. For example, Microsoft sends monthly notices of available updates. These notifications are sent to software users but are often monitored by hackers too. Hackers will use this information to seek out users who have not yet applied the updates, which provides a window to exploit software vulnerabilities.

Data Breach Consequences: Beyond the Headlines

When a breach is discovered, the first course of action is typically to stop operations until the source is identified and the issue is resolved. Yet for public agencies that provide essential services, shutting down operations may not be an option. If it is, the consequences could be detrimental to the communities served.

According to one study, the average cost of a data breach—at $3.86 million—far exceeds the cost to properly train staff and implement the internal controls necessary to help protect an organization. And a data breach often includes the following non-budgetary "costs:"

- **Damage to Your Reputation:** Building and maintaining a reputation is something that takes a lot of work, and a data breach can quickly tarnish a good reputation that has taken years to build. Forty-six percent of organizations say they suffered damage to their reputations because of data breaches.
- **Lost Trust:** Governments are responsible for all types of sensitive information. When a data breach occurs, both the public and policymakers may question the trust they had placed in that particular organization. Loss of trust can also come from how an organization responds to a breach.

What Can You Do to Avoid a Data Breach?

Unfortunately there is no way to prevent hackers from targeting your organization; however, you can establish "data hygiene" protocols to help mitigate the risk of a breach happening to you.

- **Employee Awareness, Training, and Testing:** Not understanding security risks or best practices is the root of vulnerability for organizations. Teaching employees how to recognize signs of possible fraud and how to respond appropriately is the first step toward preventing cyberattacks that may lead to a data

(Continued on page 7)

(Continued from page 6)

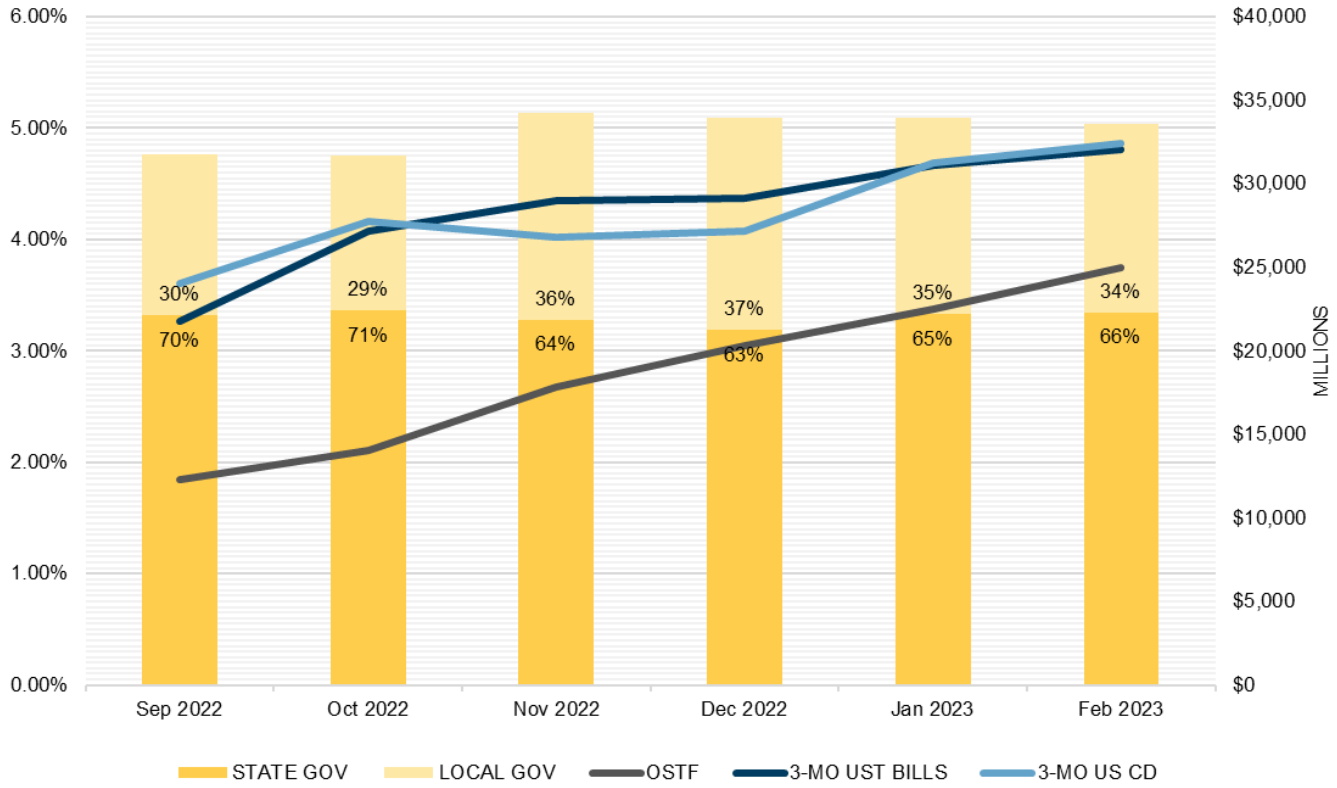
breach. Employees should understand appropriate data retention and disposal methods, use strong passwords and multi-factor authentication, understand the process for processing and responding to requests for information, and know their roles as part of their organization's incident response plan.

- Many data breaches are caused by improper disposal of records and equipment. Proper disposal can come in the form of employing a shredding service or properly "cleaning" machines before returning or disposing of them.
- Requiring passwords to meet specific criteria and implementing multi-factor authentication for online account access can also help prevent a data breach. Best practice is for passwords to be as long as permissible; contain a mix of upper and lowercase letters, numbers and special characters; and never include personal information like birthdays, street names, or pets' names. Multi-factor authentication should also always be used when available. Though not fool-proof, multi-factor authentication greatly decreases the chance of accounts being compromised and helps to ensure that only authorized individuals are accessing protected systems and information.
- An incident response plan is an organized approach to addressing the aftermath of a security breach or cyberattack. Plans should address a situation in a manner that limits damage and reduces recovery time and costs. Without a plan in place, an organization may not be able to detect an attack or follow the proper protocol to contain the incident and recover from it.

- **Apply Technical Controls and Protection Software:** Organizations should have a routine process for distributing and installing critical security patches. They should also have trained security professionals who understand the vulnerabilities of their systems and can take proactive steps to mitigate risks. Utilizing intrusion detection systems (IDS) and intrusion prevention systems (IPS) can help to detect unusual activity behind the scenes to alert IT staff to potential cyberattacks. When alerted to a potential threat, IPS can deploy prevention tactics to fight against the attack and keep protected information secure. It is also best practice to run regular upgrades to outdated or unsupported software. Routine software upgrades apply new security patches to existing software to protect against newly discovered vulnerabilities. It is important to be aware of and to manage system vulnerabilities to ensure necessary upgrades are occurring. Vulnerability management helps to ensure software patches are in place.
- **Penetration Tests:** Employing security companies to "test" the security of your organization's network is another way to help prevent data breaches. Penetration testing, also known as ethical hacking, is the practice of testing a computer system or network to detect security vulnerabilities. These tests are performed to see if an organization's network is hackable. If an area of exploit exists, it can be quickly identified and resolved as a result of this type of testing.

Operating in a digital environment challenges us daily to stay one step ahead of cybercriminals who want to exploit our protected information. Attacks continue to become more sophisticated and have required organizations to develop prevention measures that are equally sophisticated. Understanding how and why data breaches occur is the first line of defense. With the right mix of training, technical controls, and prevention software, organizations can fight back to protect their information and reduce their chance of becoming the next major security breach headline in the news.

Oregon Short Term Fund Analysis



	Sep 2022	Oct 2022	Nov 2022	Dec 2022	Jan 2023	Feb 2023
TOTAL OSTF AVG DOLLARS INVESTED (MM)	31,769	31,678	34,249	33,966	33,929	33,603
STATE GOV PORTION (MM)	22,114	22,414	21,845	21,249	22,185	22,282
LOCAL GOV PORTION (MM)	9,655	9,264	12,404	12,717	11,744	11,321
OSTF ANNUAL YIELD (ACT/ACT)	1.84	2.10	2.68	3.04	3.37	3.75
3-MO UST BILLS (BOND EQ YLD)	3.270	4.074	4.349	4.374	4.665	4.812
3-MO US CD (ACT/360)*	3.61	4.16	4.02	4.07	4.69	4.86

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 respectively) bank certificates of deposit and are quoted on a CD equivalent yield basis.

Market Data Table

	2/28/2023	1 Month	3 Months	12 Months		2/28/2023	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	4.39	4.22	3.56	0.02	Bloomberg Barclays 1-3 Year Corporate YTW*	5.40	4.81	5.02	1.94
30-Day Agy Nt Disc**	4.53	4.44	3.91	0.07	Bloomberg Barclays 1-3 Year Corporate OAS*	0.64	0.62	0.72	0.62
90-Day Agy Nt Disc**	4.74	4.61	4.30	0.34	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.86	1.85	1.88	1.87
180-Day Agy Nt Disc**	4.95	4.69	4.49	0.42					
360-Day Agy Nt Disc**	5.02	4.83	4.87	2.34	7-Day Muni VRDN Yield**	3.42	1.66	1.85	0.20
					O/N GGC Repo Yield**	4.59	4.35	3.82	0.06
30-Day Treasury Bill**	4.35	4.35	3.71	0.04					
60-Day Treasury Bill**	4.56	4.44	3.94	0.18	Secured Overnight Funding Rate (SOFR)**	4.55	4.31	3.82	0.05
90-Day Treasury Bill**	4.67	4.51	4.14	0.32					
6-Month Treasury Yield**	5.15	4.83	4.68	0.64	US 10 Year Inflation Break-Even**	2.38	2.25	2.37	2.62
1-Year Treasury Yield**	5.01	4.67	4.71	0.99					
2-Year Treasury Yield**	4.82	4.20	4.31	1.43	1-Day CP (A1/P1)**	4.51	4.47	3.77	0.08
3-Year Treasury Yield**	4.53	3.90	4.05	1.63	7-Day CP (A1/P1)**	4.53	4.48	3.79	0.08
					30-Day CP (A1/P1)**	4.58	4.54	4.02	0.24
1-Month LIBOR**	4.67	4.57	4.14	0.24					
3-Month LIBOR**	4.97	4.81	4.78	0.50	30-Day CD (A1/P1)**	4.65	4.60	4.04	0.21
6-Month LIBOR**	5.26	5.10	5.20	0.80	90-Day CD (A1/P1)**	4.94	4.79	4.62	0.53
12-Month LIBOR**	5.68	5.34	5.57	1.29	6-Month CD (A1/P1)**	5.21	5.01	5.10	0.82
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	5.41	5.20	5.38	1.26

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