September 2022

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Market Update

This reporting period marks one of the most volatile quarters in the bond market since the Paul Volker–led era of the Federal Reserve in the early 1980s. The first half of 2022 saw the 10-year Treasury note yield rising from 1.8% to 3.0%, and what some are calling the worst year for Treasurys in history. From June to August, the 10-year note vacillated between 2.5% and 3.5%, which reflected less a trading band and more a market with zero convictions. The short-end continued to sell off during the reporting period, with the 2-year note moving a comparably straight direction from 2.5% to 3.5%.

The net result is an inverted yield curve with tendency to invert further on data releases or comments from members of the Fed's Board of Governors. Chairman Powell remains "data dependent" and is offering little in the way of long-term forward projections/guidance on this cycle's peak federal funds level. Daily trading has thus devolved to whether the day's macro release points to recession or soft landing.

The labor market remains strong with the September unemployment rate at 3.7%, up from 3.5% in August—comparable levels to 2019's red -hot jobs market. The July Consumer Price Index (CPI) has moderated to 8.5% year-over-year, down from 9.1% in June but still

(Continued on page 2)

Interest Rates

Average Annualized Yield	
August	1.5774%

Interest Rates	
August 1–9	1.40%
August 10–31	1.65%

Upcoming Holiday

The pool will be closed on Monday, October 10, for Columbus Day. Connect will be available, but the system will not allow transactions to settle on the holiday.

(Continued from page 1)

the highest rate since December 1981 (see chart on page 3). Forecasters are starting to cut year-end inflation projections, both because of the base year effects but also due to pressure coming off key commodities.

After nearly a year of sustained price increases, most commodities are either trending down or holding current levels. Oil is down to approximately $88 per barrel from the June peak of $114. Natural gas remains elevated from the continuing conflict in Eastern Europe at approximately $8 per btu, double the price from the start of year. Industrial metals are seeing a slump due to weakness in the Chinese real estate market, with copper off 25% from the second quarter peak. The grain complex is more mixed with wheat trending down and corn prices increasing.

Gold continues to underwhelm as an inflation hedge, pulling back from a peak at about $2,000 per ounce before falling back to near $1,700. The cause here is the incredible run by the dollar. The yen has given up 25% value to the dollar due to the Japanese central bank maintaining a loose monetary policy. Meanwhile, the euro finally breached parity with the dollar, a 12% loss of value from the start of the year.

As alluded above, the Eurozone continues to struggle with energy concerns and potential shortages of natural gas going into winter, particularly in the event of a colder-than-average winter. Moreover, the European Central Bank is stuck in an unenviable situation of having to reduce inflation, while trying to keep the sovereign bonds of member states from decoupling.

Oregon Short Term Fund

The OSTF's paid rate was raised on September 8 from 1.65% to 1.90%. The fund's 47% allocation to floating rate securities (up from 45% as of June 30), benchmarked primarily to 3-month Treasury Bills, Secured Overnight Financing Rate (SOFR), and Libor, will keep pace with the trend in short-term rates and, with three remaining meetings of the Federal Open Market Committee in 2022 and total hikes of 150 to 175 basis points, staff expects additional upward revisions to the paid rate in the near future. Should you have questions, contact members of the Fixed Income Team at 503.431.7900.

Impact on Markets from June 2022 through August 2022

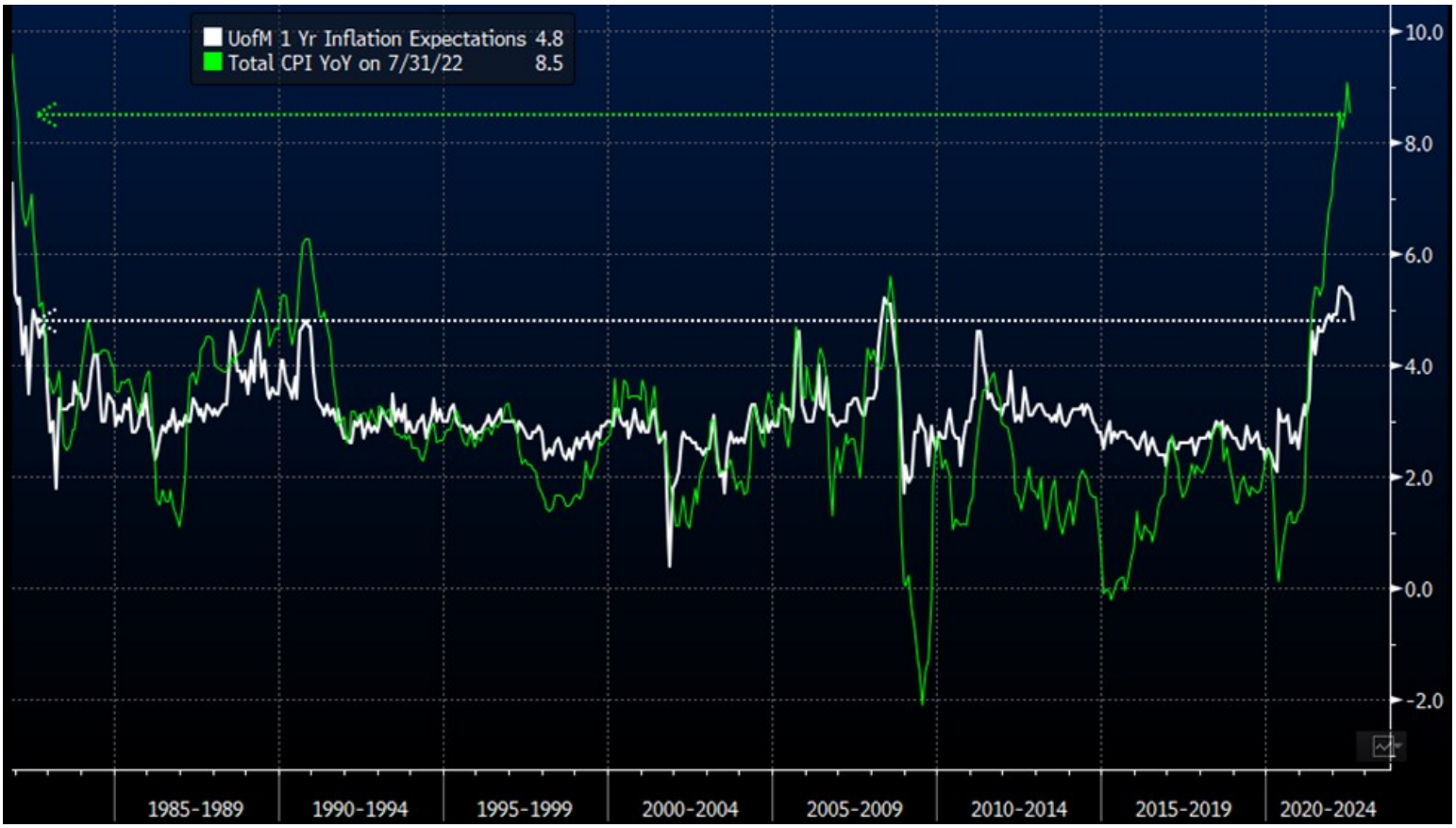
	6/30/2022	8/31/2022	Delta	Highlights
S&P 500	3,785	3,955	+4.8%*	Intraday low: 3,722 on 7/14
30-Year Treasury	3.185	3.294	+10.9 bps -2.30%*	Intraday low: 2.852 on 8/2
10-Year Treasury	3.016	3.195	+17.9 bps -0.96%*	Intraday low: 2.521 on 8/2
2-Year Treasury	2.957	3.495	+53.8 bps -0.53%*	Intraday low: 2.725 on 7/1
3-Month Bills	1.667	2.925	+125.8 bps +0.21%*	Intraday low: 1.611 on 7/1

**Total Return (dividends reinvested for S&P; price and income for Treasurys)*

(Continued on page 3)

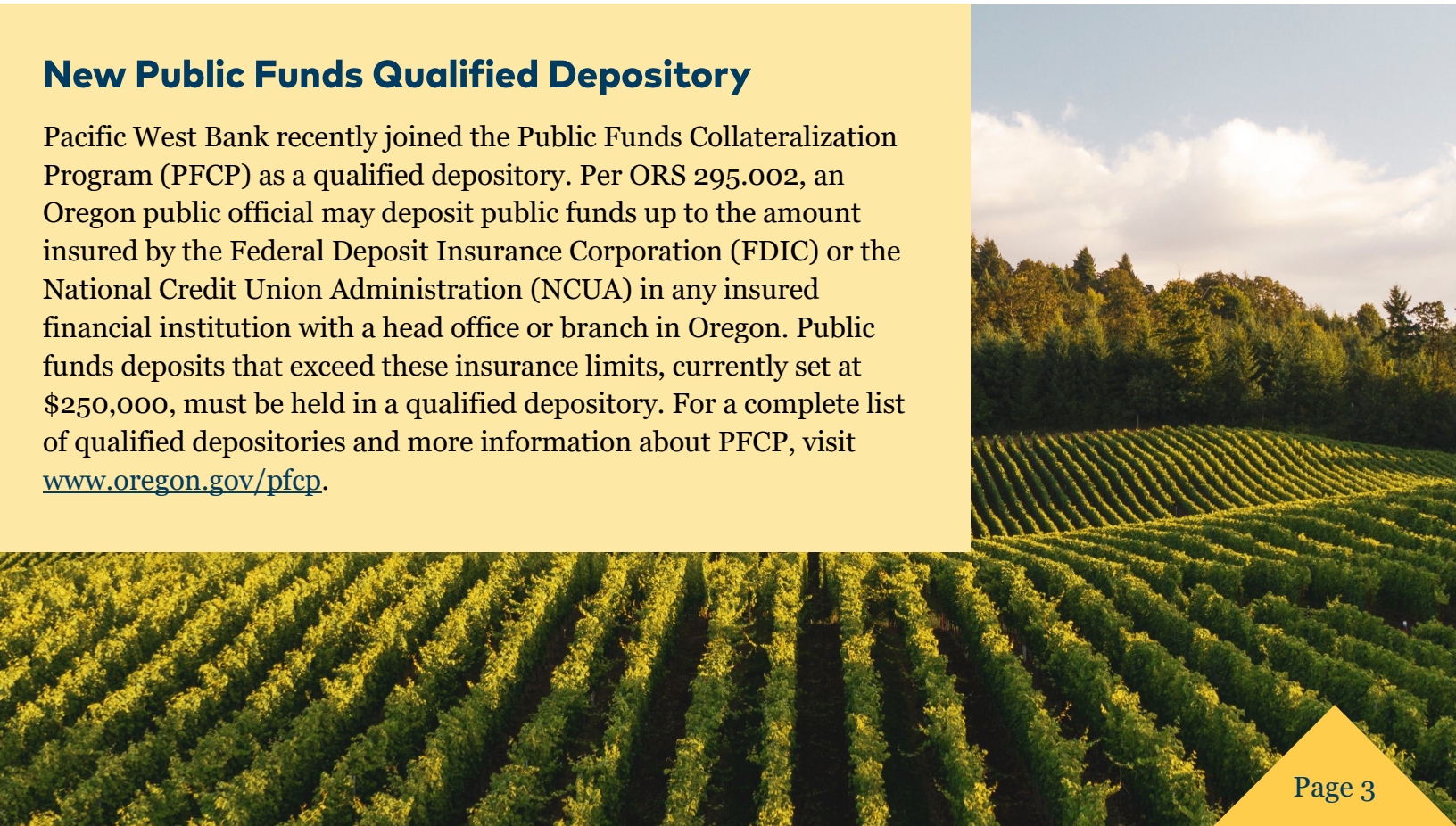
(Continued from page 2)

Consumer Price Inflation and 1-year Inflation Expectations at highest levels since 1981



New Public Funds Qualified Depository

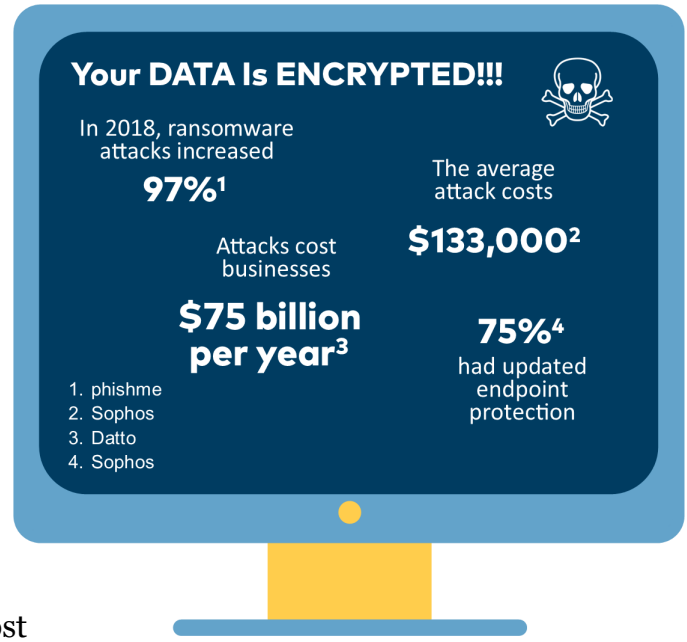
Pacific West Bank recently joined the Public Funds Collateralization Program (PFCP) as a qualified depository. Per ORS 295.002, an Oregon public official may deposit public funds up to the amount insured by the Federal Deposit Insurance Corporation (FDIC) or the National Credit Union Administration (NCUA) in any insured financial institution with a head office or branch in Oregon. Public funds deposits that exceed these insurance limits, currently set at $250,000, must be held in a qualified depository. For a complete list of qualified depositories and more information about PFCP, visit www.oregon.gov/pfcp.



Security Spotlight: Ransomware

Ransomware is a type of malicious software designed to make files and systems inaccessible to the rightful owner in order to demand a price, or "ransom," for restoring access. It can take advantage of the myriad of ways hackers gain illicit access of computing devices.

- **Phishing Attacks:** An e-mail using social engineering techniques to influence a user to click a link or run a program.
- **Trojan Horses:** Viruses that are embedded or disguised within innocuous programs or even seemingly necessary software that an unwitting user runs on their machine.
- **Worms:** A self-replicating program that moves through computer networks. Unlike the methods above, a worm does not depend on tricking users—all this form of ransomware needs is a device to access an infected network.
- **Hacking Weak Passwords:** Described as using "brute force attacks," this type of hacking uses a program to try common passwords until one works. This approach may seem like a fool's errand, however, it is actually simply a numbers game. Careless or simple passwords and poor network security features can turn an impossibility into an inevitability.



- **Networking Vulnerabilities:** Some of the biggest, most newsworthy attacks have been launched through vulnerabilities identified by hackers related to missing operating system patches, outdated software releases, misconfigured firewalls, and the use of default passwords.

Unlike other types of malicious attacks (spyware, phishing, etc.), ransomware will make itself known. Usually, there is a pop-up informing the user that their data has been taken hostage. There may be a countdown clock, a description of how the data has been made inaccessible, and what the user may need to do to get it back.

Invariably, there is a price requested and instructions for how to pay it. The most frequent demand is for Bitcoin or some other cryptocurrency. However, gift cards, premium-rate SMS, or long distance telephone fees have also been reported. Some programs even employ negotiating tactics, such as offering some non-essential files back as a goodwill gesture, or using a tiered pricing structure based on how long it takes to pay the ransom. Ransomware attacks also often involve taking control of data and system resources used by public sector entities to deliver essential services (*e.g.*, healthcare, law enforcement, utilities, etc.), which increases the likelihood of a ransom getting paid.

Ransomware can take control of your device in many different ways, some of which include the following:

(Continued on page 5)

Reporting Unclaimed Property

Oregon's Unclaimed Property Program works to unite Oregonians with their uncashed checks, forgotten deposits and refunds, and other unclaimed money.

Oregon governments, businesses, and nonprofits are doing their part, too. Each year, organizations in Oregon do their best to reach out to customers and contacts who may have unclaimed property. If those people can't be reached, the organizations then itemize and report any unclaimed funds to the state.

Oregon's annual unclaimed property reporting window runs from October 1 to November 1. All Oregon businesses—no matter how big or small they are—are required by law to report unclaimed funds to the state during the window. The same goes for state agencies, local governments, and nonprofits that hold unclaimed property.

Organizations can even report *incidental* unclaimed property for other states to Oregon unless having received specific instructions to report from the other state. Incidental property is no more than 10 items totaling $1000 or less for any state. *Note that an organization may be charged penalties and/or interest by the other state.*

After organizations report and remit unclaimed property to the state, the funds are held by Treasury in perpetuity. Oregonians can search for their names at unclaimed.oregon.gov to see if they are entitled to any unclaimed funds.

Learning how to report unclaimed property is just as easy. Treasury's Unclaimed Property website has information about reporting requirements, holding periods for different types of property, and instructions for requesting a reporting extension.

We welcome your questions about Oregon's Unclaimed Property Program. Visit unclaimed.oregon.gov/app/contact-us to reach out to staff. And spread the word to your employees and customers that a quick search at unclaimed.oregon.gov can help them see if Oregon is holding unclaimed property that belongs to them.

(Continued from page 4)

- A **Blocker** is a program that inhibits your ability to use the infected device. It could be a browser window that cannot be closed through the usual means, a fake software update window that demands action, a fake message from a law enforcement agency, or a program that floods the screen with unwanted images.
- **Encryption** is a technology that scrambles data to protect it from being read by anyone except those with the "key." The key is usually a random string of alphanumeric characters. Some forms of encryption can be reversed, but not without significant time and cost that is often beyond the value of the data. For this reason, blockers often claim encryption even if the data is not actually encrypted.
- **Leakware** is a form of ransomware that threatens to release sensitive information publicly instead of inhibiting access.

How Big of a Problem Is This Really?

According to industry experts, the damages caused by ransomware attacks have increased. This is partly due to hackers getting better at targeting institutions and organizations directly, especially those that have the resources to pay larger ransoms. In other words, your personal computer is less likely to be targeted or taken "hostage," but your work files could be a prized objective for cybercriminals.

(Continued on page 6)

(Continued from page 5)

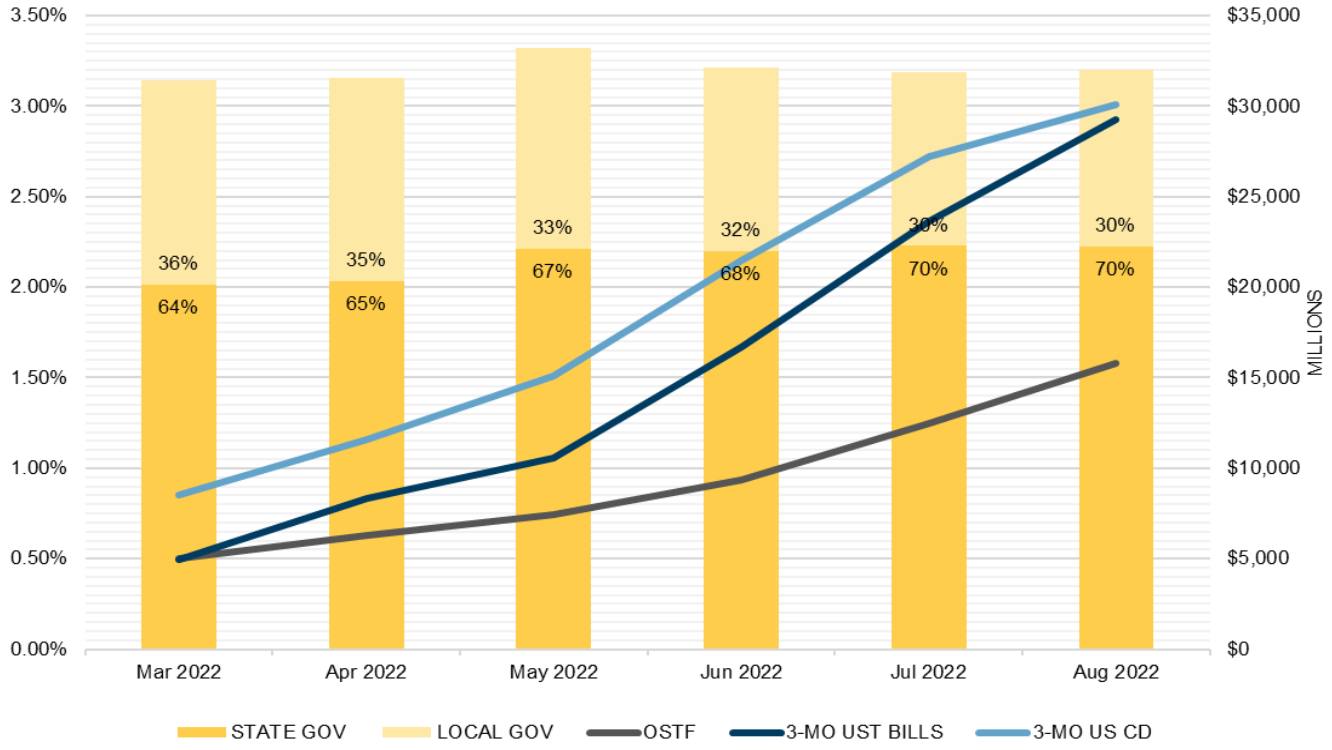
It is also important to note that the damages of a ransomware attack go well beyond the actual ransom—in fact, paying the ransom could be only the beginning. A ransomware attack can cost an organization millions in lost productivity and reputational damages, not to mention the time and resources it could take to get affected systems in working order again.

One reported attack on a large municipality was estimated to cost close to $17 million. That price tag may make it seem like a necessity to pay a few thousand in Bitcoin and move on. However, according to a survey conducted by betanews.com, paying the ransom resulted in the stolen files being returned only 26% of the time. Another source suggests the number is closer to 40%, but it underscores the point that there are often no easy answers to ransomware attacks once they have succeeded in locking users out. The good news is that there are ways to help prevent these kind of attacks.

- **Spam filters** can stop many attack e-mails, especially if they carry suspicious attachments, links, etc. Unfortunately, it takes only one e-mail to get through to cause significant damage. Therefore, end-users must be vigilant as well, understanding the risks associated with clicking on unknown links and downloading attachments. It is important for everyone to understand the current cyber risks that exist and their role in helping to avoid potential breaches, and to protect against cyber threats like ransomware. Nowadays, it is more likely you will need to use your cyber safety training than fire safety or medical emergency training.
- **Antivirus software** also plays an important role in protecting against ransomware, since it is a type of malware. While antivirus software may not prevent the next big breach, if kept up-to-date, it can be a good way to protect against more well-known forms of malware. To keep antivirus software and signatures up-to-date, it is recommended that regular computer scans be conducted.
- **Vigilance** applies to information technology processes and professionals as well. Some of the largest ransomware attacks took place after the weakness in a common operating system was already identified and a security patch was made available. A notable example of this is the WannaCry ransomware worm, which wrought an estimated $4 billion in damages by exploiting a loophole that was patched weeks before the worm became widespread. All 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 system and can take proactive steps to mitigate the risks.
- A **back-up system** that is largely independent from the regular network that users operate on a daily basis is one of the chief ways to mitigate ransomware risk. The separation is needed to ensure that a ransomware attack does not infect the back-up as well. Installing a back-up system will not prevent a cybersecurity threat, but it is a process that can make an attack less damaging, especially if ransomware is identified quickly.

Ransomware attacks have become a major feature of the cyber threat landscape for institutions of all sizes. Like phishing and social engineering attacks, it is no longer a question of whether or even when, but rather of how many attacks institutions will be exposed to on a daily basis. While the most sophisticated attacks may require equally sophisticated prevention measures, the majority can be avoided with widely available technology, a well-thought-out institutional approach to networks and data protection, and end-user education.

Oregon Short Term Fund Analysis



	Mar 2022	Apr 2022	May 2022	Jun 2022	Jul 2022	Aug 2022
TOTAL OSTF AVG DOLLARS INVESTED (MM)	31,437	31,534	33,245	32,158	31,884	31,978
STATE GOV PORTION (MM)	20,147	20,340	22,145	21,998	22,297	22,255
LOCAL GOV PORTION (MM)	11,290	11,194	11,100	10,160	9,587	9,723
OSTF ANNUAL YIELD (ACT/ACT)	0.50	0.63	0.75	0.93	1.25	1.58
3-MO UST BILLS (BOND EQ YLD)	0.496	0.834	1.058	1.667	2.364	2.925
3-MO US CD (ACT/360)*	0.85	1.16	1.51	2.15	2.72	3.01

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

	8/31/2022	1 Month	3 Months	12 Months		8/31/2022	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	2.18	1.81	0.57	0.01	Bloomberg Barclays 1-3 Year Corporate YTW*	4.16	3.61	3.17	0.50
30-Day Agy Nt Disc**	2.35	2.16	0.72	0.01	Bloomberg Barclays 1-3 Year Corporate OAS*	0.76	0.80	0.73	0.33
90-Day Agy Nt Disc**	2.90	2.52	1.15	0.03	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.93	1.95	1.97	1.83
180-Day Agy Nt Disc**	3.22	2.89	1.40	0.03					
360-Day Agy Nt Disc**	2.74	2.74	2.07	0.02	7-Day Muni VRDN Yield**	1.50	1.33	0.79	0.02
					O/N GGC Repo Yield**	2.28	2.32	0.81	0.06
30-Day Treasury Bill**	2.02	2.09	0.64	0.02					
60-Day Treasury Bill**	2.50	2.17	0.86	0.03	Secured Overnight Funding Rate (SOFR)**	2.29	2.27	0.79	0.05
90-Day Treasury Bill**	2.77	2.36	1.06	0.03					
6-Month Treasury Yield**	3.35	2.86	1.57	0.05	US 10 Year Inflation Break-Even**	2.48	2.55	2.65	2.34
1-Year Treasury Yield**	3.51	2.94	2.07	0.07					
2-Year Treasury Yield**	3.50	2.89	2.56	0.21	1-Day CP (A1/P1)**	2.30	1.54	0.74	0.14
3-Year Treasury Yield**	3.52	2.81	2.73	0.41	7-Day CP (A1/P1)**	2.25	2.30	0.77	0.12
					30-Day CP (A1/P1)**	2.42	2.35	1.04	0.09
1-Month LIBOR**	2.55	2.36	1.12	0.08					
3-Month LIBOR**	3.10	2.79	1.61	0.12	30-Day CD (A1/P1)**	2.51	2.33	1.04	0.08
6-Month LIBOR**	3.66	3.33	2.11	0.15	90-Day CD (A1/P1)**	3.06	2.73	1.46	0.11
12-Month LIBOR**	4.22	3.71	2.74	0.23	6-Month CD (A1/P1)**	3.60	3.32	2.01	0.15
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	3.81	2.95	2.80	0.21

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

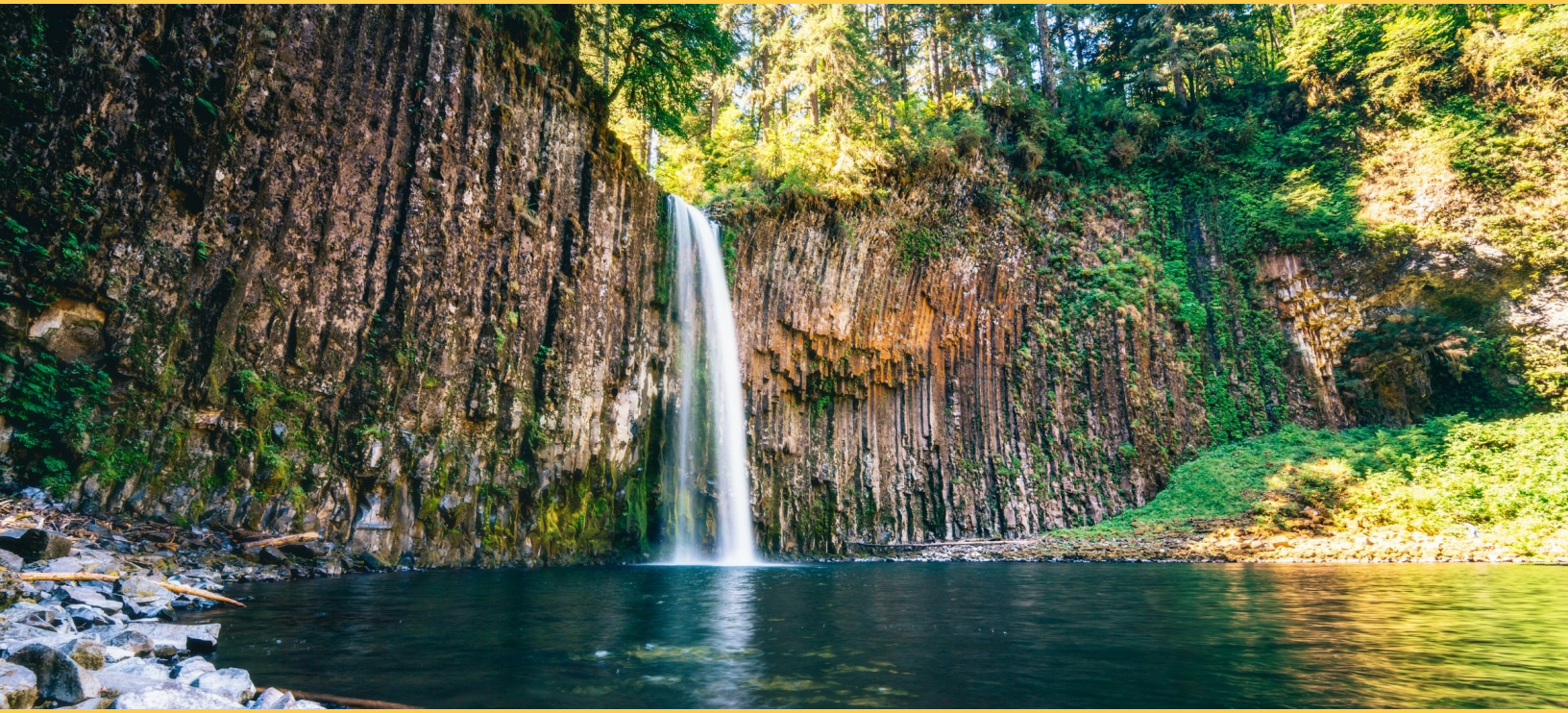
- Connect Access
- Transactions
- Reporting
- Account/User Maintenance
- Eligibility

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