May 2024

OREGON STATE TREASURY

Inside the Vault

Local Government Edition

Security Spotlight: Vendor E-mail Compromise

You receive what you believe is an e-mail from one of your vendors a couple of weeks prior to a deadline for payment of services rendered. This e-mail provides you with new instructions on where and how you should submit the payment. What do you do?

- *Update your records with the new information right away—you really like this vendor and want to demonstrate a good payment history as you want to work with them in the future.*
- *Call the sender based on the contact information in the e-mail that was JUST sent to you to verify the update and, once verified, update your systems accordingly.*
- *Call a vendor contact based on information you previously received to verify the requested change and, if verified, update your systems accordingly.*

What Is Vendor E-mail Compromise?

Recently, an attack known as "vendor e-mail compromise" has become more popular and more effective. Vendor e-mail compromise is when criminals use lookalike domains or e-mail spoofing techniques to trick your employees into thinking that they are

(Continued on page 2)

Interest Rates

Average Annualized Yield

April	5.20%

Interest Rates

April 1–30	5.20%

Upcoming Holiday

The pool will be closed on Monday, May 27, for Memorial Day. Connect will be available, but the system will not allow transactions to settle on the holiday.

(Continued from page 1)

communicating with a trusted contact at a vendor they communicate with on a regular basis. This may prompt employees to reveal sensitive information, submit payment to unauthorized parties, or give unauthorized access to your network.

E-mails that appear to come from a trusted source, such as a vendor contact, result in an employee being more likely to consider these e-mails as legitimate, and they may respond, click on links, and open attachments, rather than mark the e-mails as spam or junk or delete them.

How Can You Guard against This Attack?

A large part of cybersecurity is employee awareness and education. This can help protect organizations from vendor e-mail compromise, in addition to phishing attempts, business e-mail compromise, and other social engineering attacks. By providing employees with tips to spot or prevent an attack through commonsense methods, your organization can avoid falling prey to an attack:

- Check the domain name in the sender's e-mail address to help ensure it was sent from a trusted source. Common tricks for lookalike domains include using a zero (0) instead of the letter "O," using the letters "rn" instead of "m," and using a capital "I" in place of a lower case "l."
- Confirm the e-mail with a trusted contact *before* taking any action. Call a vendor contact based on information you *previously* received from the vendor to verify the requested change and, if verified, update your systems accordingly. (Correct answer to "What do you do?" from above.)
- Use multi-factor authentication whenever possible, especially for sensitive accounts or money movement.
- Focus on looking for anything suspicious or out-of-the-ordinary such as a sudden business protocol change, sense of urgency, or typos.
- Do not click links in e-mails. Instead, visit the vendor's website and log into your account from that site. This helps to ensure you are accessing the correct website.

What Can You Do If You Fall Victim to a Vendor E-mail Compromise Attack?

If you or an employee fall victim to a vendor e-mail compromise attack, there are a few measures your organization can take to try to minimize the damage (coordinate with your IT security staff and follow your organization's established procedures):

- Run anti-virus and malware scans.
- Change all passwords and security questions immediately.
- Contact the vendor to inform them of the fraud.
- Notify all financial providers and place stop payments on any payments authorized to the scammers.
- Contact law enforcement to report the incident.
- Conduct post-incident cybersecurity training.

Although nothing is foolproof, and even the most rigorous cybersecurity program may still be at risk for cybersecurity attacks, promoting employee awareness and education on topics like vendor e-mail compromise attacks can help reduce the risk of a cybersecurity attack.

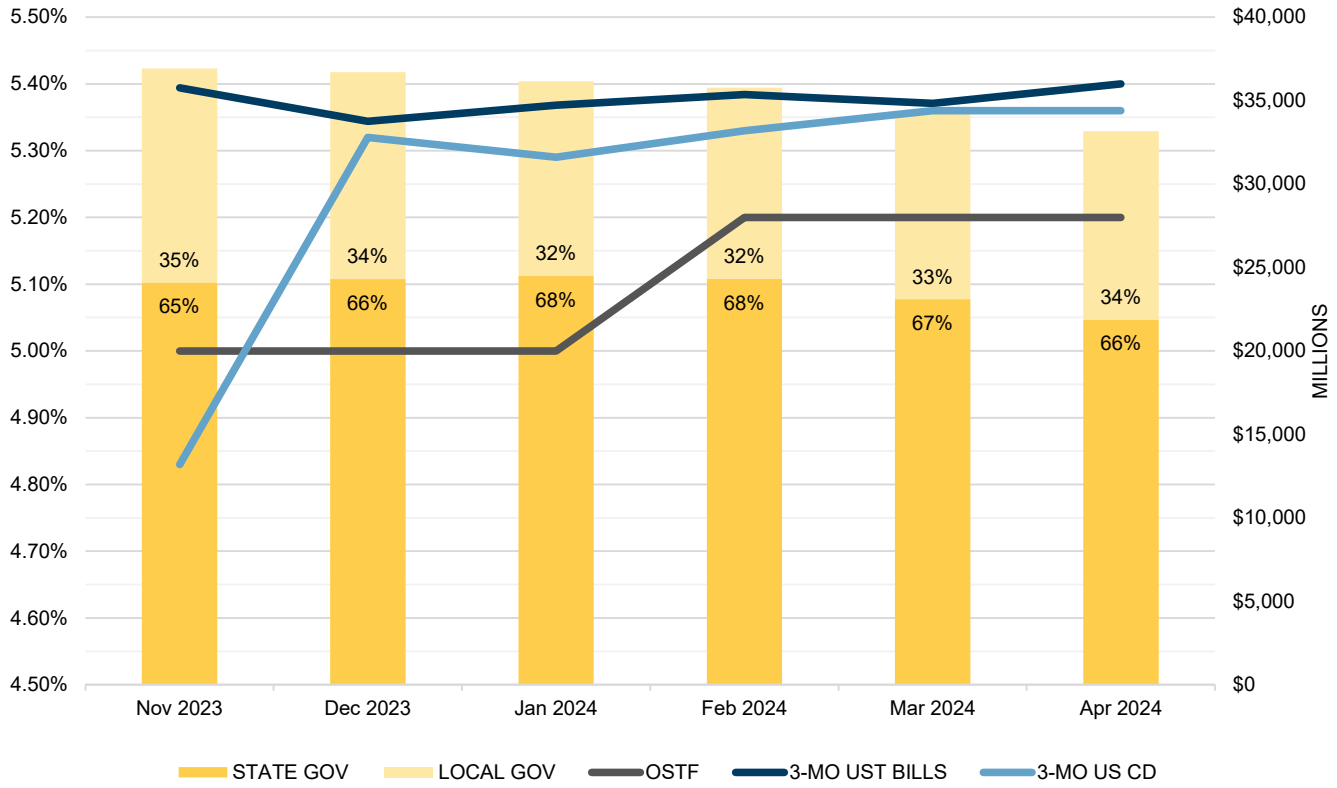
LGIP Redemptions: Wire Transfer vs. ACH

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 csgmww@pfmam.com if you have questions about which redemption option best meets your needs.

Oregon Short Term Fund Analysis



	Nov 2023	Dec 2023	Jan 2024	Feb 2024	Mar 2024	Apr 2024
TOTAL OSTF AVG DOLLARS INVESTED (MM)	36,918	36,700	36,151	35,766	34,381	33,164
STATE GOV PORTION (MM)	24,110	24,315	24,493	24,316	23,097	21,878
LOCAL GOV PORTION (MM)	12,808	12,385	11,658	11,450	11,284	11,286
OSTF ANNUAL YIELD (ACT/ACT)	5.00	5.00	5.00	5.20	5.20	5.20
3-MO UST BILLS (BOND EQ YLD)	5.394	5.344	5.368	5.384	5.371	5.400
3-MO US CD (ACT/360)*	4.83	5.32	5.29	5.33	5.36	5.36

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

	4/30/2024	1 Month	3 Months	12 Months		4/30/2024	1 Month	3 Months	12 Months
7-Day Agency Discount Note**	5.25	5.11	5.18	4.56	Bloomberg Barclays 1-3 Year Corporate YTW*	5.57	5.21	4.93	4.96
30-Day Agy Nt Disc**	5.24	5.21	5.19	4.65	Bloomberg Barclays 1-3 Year Corporate OAS*	0.54	0.57	0.66	0.92
90-Day Agy Nt Disc**	5.18	5.18	5.16	4.87	Bloomberg Barclays 1-3 Year Corporate Modified Duration*	1.84	1.81	1.76	1.87
180-Day Agy Nt Disc**	5.11	5.05	4.90	4.89					
360-Day Agy Nt Disc**	4.96	4.78	4.52	4.82	7-Day Muni VRDN Yield**	3.77	3.64	3.74	3.86
					O/N GGC Repo Yield**	5.43	5.39	5.38	4.81
30-Day Treasury Bill**	5.27	5.25	5.26	4.03					
60-Day Treasury Bill**	5.29	5.27	5.25	4.79	Secured Overnight Funding Rate (SOFR)**	5.34	5.34	5.32	4.81
90-Day Treasury Bill**	5.29	5.26	5.23	4.95					
6-Month Treasury Yield**	5.40	5.32	5.20	5.02	US 10 Year Inflation Break-Even**	2.40	2.32	2.25	2.21
1-Year Treasury Yield**	5.24	5.03	4.72	4.76					
2-Year Treasury Yield**	5.04	4.62	4.21	4.01	1-Day CP (A1/P1)**	5.30	5.34	5.30	4.79
3-Year Treasury Yield**	4.88	4.41	3.98	3.72	7-Day CP (A1/P1)**	5.32	5.34	5.31	4.83
					30-Day CP (A1/P1)**	5.35	5.37	5.35	4.98
1-Month SOFR**	5.32	5.33	5.33	5.02					
3-Month SOFR**	5.33	5.30	5.32	5.08	30-Day CD (A1/P1)**	5.37	5.44	5.38	5.09
6-Month SOFR**	5.31	5.22	5.17	5.08	90-Day CD (A1/P1)**	5.46	5.41	5.43	5.28
12-Month SOFR**	5.23	5.00	4.83	4.81	6-Month CD (A1/P1)**	5.49	5.45	5.32	5.38
Sources: *Bloomberg Index Services, **Bloomberg					1-Year CD (A1/P1)**	5.57	5.23	5.14	5.35

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
csgmww@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