October 2020

OREGON STATE TREASURY

Inside the Vault

State Agency Edition

National Cybersecurity Awareness Month

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

Due to Veterans Day, Treasury, the Federal Reserve, and Oregon banks will be closed on Wednesday, November 11. Customer statements and files will not be produced for November 11 due to the closures. In addition, ACH files sent to Treasury after the deadline on Tuesday, November 10, will be sent to the bank on Thursday, November 12, and must have an effective date of November 13 or later.

Interest Rates

Average Annualized Yield

September	1.00%

Interest Rates

September 1–30	1.00%

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.

Data Security Reminder

It is becoming more commonplace for major retailers, restaurants, and government organizations to announce a data security breach. While each breach is unique, each results in the possibility of data being compromised. Such data can include credit card numbers, bank account information, social security numbers, or other personally identifiable information. Since most agencies transmit, process, or store this same information in electronic or physical format, it is vitally important for agencies to be diligent about keeping data security at the forefront of business decisions and processes.

As a reminder, in addition to the Payment Card Industry Data Security Standard (PCI DSS) and Nacha Rules, agencies are required to comply with Office of the State Chief Information Officer policies, Oregon Accounting Manual Chapter 10, as well as Treasury Cash Management Policies. Please check in with your agency's security team, CFO, or manager responsible for financial controls about the status of your organization's compliance with such requirements as they may reduce the risk of a data breach.

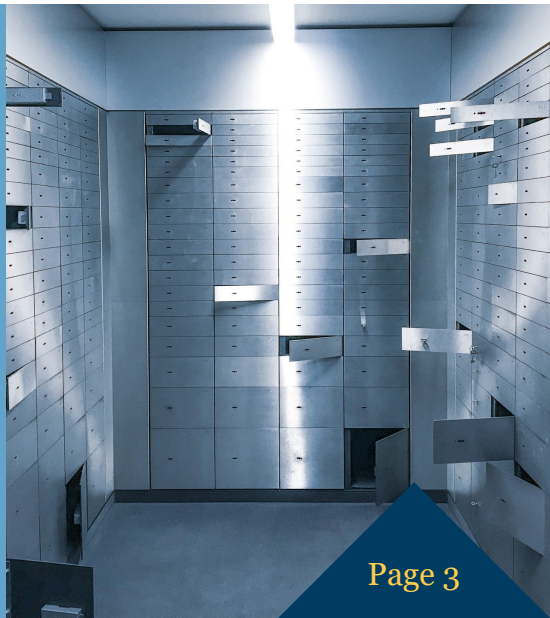
Below are a few recurring themes included in many regulatory requirements that are intended to help safeguard sensitive information:

- Maintain updated data security policies and procedures that are aligned with applicable regulatory requirements.
- Ensure that agency management and staff are aware of your organization's liabilities and responsibilities for protecting sensitive information when processing payments including merchant cards, ACH transactions, and onsite electronic deposits.
- Provide training to staff, at least annually, about the data security policies and procedures applicable to their duties.
- Re-evaluate the reason for storing personally identifiable information.

These are but a few reminders about protecting your customers' personally identifiable information. If you have questions about the regulatory requirements for any of the banking services used by your organization, contact Customer Solutions at customersolutions@ost.state.or.us.

Service Spotlight

Safekeeping is a free service that allows agencies to store items of value in Treasury's vaults. Items placed in safekeeping are usually being held to insure performance, cover a liability, or provide some other means of financial protection. Items placed in safekeeping are inventoried and agencies receive a receipt for each item. Agencies must submit a written request to retrieve items from safekeeping and items must be picked up in person. If you are interested in safekeeping, or have questions regarding cash management services generally, contact Customer Solutions at customersolutions@ost.state.or.us.



U.S. Bank Permanently Closing Branches

On November 1, U.S. Bank will permanently close 26 branches across Oregon with six more branches closing January 2, 2021. The closures are part of a plan originally announced in 2019 to optimize its branch footprint due to the shift toward digital banking. Agencies impacted by the branch closures should contact Edie Kessel, Banking Operations Manager, at 503.373.1897.

Portland-Area Branches

- 160th & Division
- 4th & Harrison
- 67th & Glisan
- Citizens
- Clackamas Town Center
- Cornelius Pass Albertsons
- East Gresham
- Emanuel Hospital
- Forest Grove
- Gladstone
- Hillsboro
- John's Landing
- Menlo Park
- Milwaukie Safeway
- Mt. Hood CC
- North Beaverton
- N. Interstate Fred Meyer
- Oregon City
- Sherwood Walmart
- Tigard
- Troutdale Albertsons
- Washington Square*
- Woodstock Blvd

Other Oregon Branches

- Albany (205 Ellsworth)*
- Coquille Valley*
- Elgin*
- Eugene (Coburg Crescent)*
- Eugene (7th & Chambers)
- Jacksonville
- Klamath Falls (740 Main)
- Medford (Rogue Valley Manor)
- Myrtle Creek*

**Branch will close January 2, 2021*

ACH and Merchant Card Risk Assessments

The annual deadline for completion of both ACH Risk Assessments and Payment Card Industry Data Security Standard (PCI DSS) Self-Assessment Questionnaires (SAQs) is December 31. Treasury recently sent instructions for the ACH assessment to agency ACH contacts. If you are an ACH contact and did not receive an e-mail, contact Customer Solutions at customersolutions@ost.state.or.us with your agency name and contact information.

Treasury is working with certain agencies to pilot Elavon's PCI Compliance Manager to complete SAQs (*see* Treasury policy FIN 215) but the tool will not be broadly available for use this year. Instead, agencies should follow their existing approaches to completing SAQs. If you have questions about SAQs, contact Customer Solutions. Also, Customer Solutions will soon contact agencies to assist with enrollment in PCI Compliance Manager for future use.

Spear Phishing

All organizations, including state agencies and other governmental entities, 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 and prevention strategies, 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.

Signing & Submitting Cash Management Forms

With many state employees working from home to support social distancing, Treasury recognizes that agencies may face challenges signing and submitting certain cash management forms. To assist agencies, we have revised our wire transfer and account transfer forms to accommodate electronic signatures. The revised forms, and instructions on how to complete them, are now available on our website.

Director of Finance
Cora Parker
503.378.4633

Deputy Director of Finance
Mike Auman
503.378.2752

Policy & Strategy Manager
Bryan Cruz González
503.378.3496

Cash Management Analyst
Natalya Cudahey
503.378.8256

Administrative Specialist
Kari McCaw
503.378.4633

Banking Fax
503.373.1179

Banking Operations Manager
Edie Kessel
503.373.1897

Banking Operations Coordinator
Ellis Williams
503.378.4990

ACH File Issues
ach.exception.notify@ost.state.or.us

Check Fraud/Stop Payments
Check Image Requests
Check Stock Testing
Ashley Moya
503.373.1944

Fed Wires/ACH Origination
Shannon Higgins
503.378.5043

Local Government Investment Pool
Edie Kessel
503.373.1897

Merchant Card/U.S. Bank
Nikki Main
503.378.2409

Online User
Password Resets
ost.banking@ost.state.or.us

Safekeeping/Debt Service
Sherry Hayter
503.378.2895

Customer Solutions Team
customersolutions@ost.state.or.us
503.373.7312

Analysts/Consultants
Lyndsie DeOlus
Heidi Lancaster

Cash Management Improvement & Renewal Program
cmirp@ost.state.or.us

Manager
Brady Coy
503.378.2457

Business Analyst
Angel Bringelson
503.378.5865

Contracted Project Manager (TEK Systems)
David Riffle
503.373.7864

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