April 2020

OREGON STATE TREASURY

Inside the Vault

State Agency Edition

Nacha Rule Update

On April 1, 2020, Nacha's Differentiating Unauthorized Return Reasons Rule took effect. The rule is designed to help Originating Depository Financial Institutions (ODFIs) and Originators differentiate between returns related to a consumer's claim that there was *no authorization* for a payment versus a claim that an error occurred with a *properly authorized* payment. The new rule will allow Nacha to more precisely measure the volume of unauthorized returns within the ACH network and provide Originators with the option to fix and resubmit debits that were returned for containing errors.

The new rule re-purposes Return Reason Code (R11) for use when a Receiver claims that there was an error *with an otherwise authorized entry*. Currently, Return Reason Code R10 is used as a catch-all for various types of underlying unauthorized return reasons including some for which a valid authorization exists, such as a debit on the wrong date or for the wrong amount. In these types of cases, a return of the debit still should be made but the Originator and its customer (the Receiver) might both benefit from a *correction* of the error rather

(Continued on page 2)

EFT BSR Project Update

Project staff, like many state employees, are working from home to support social distancing. Planning for the next phase of the project continues, though at a slower pace. Agency KeyHolders should look for a more detailed project update soon.

Interest Rates

Average Annualized Yield

March	2.0806%

Interest Rates

March 1–10	2.25%
March 11–31	2.00%

(Continued from page 1)

than the termination of the original authorization. The use of (R11) enables a return that conveys this new meaning of "error" rather than "unauthorized."

Nacha has updated the definitions of these two Return Reason Codes:

- **R10 Customer Advises Originator is Not Known to Receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account.** This code should be used for all returns of an *unauthorized* debit to a consumer account.
- **R11 Customer Advises Entry Not in Accordance with Terms of the Authorization.** This code should be used when
  - Amount is different than that authorized by the receiver
  - Payment posted earlier then authorized by the receiver
  - Incomplete transaction (*i.e.*, a payment to an intended third-party payee that was not made or completed by the originator)
  - Improperly reinitiated entry
  - Improperly originated ARC, BOC, or POP entries.

If your agency originates ACH debits to collect payments from consumers and you have questions related to this new rule, contact Brady Coy at 503.378.2457 or at brady.coy@ost.state.or.us.

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 are revising 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.

Bank Branch Deposits

In response to the COVID-19 pandemic, banks are taking various actions to maintain operations while protecting the health of customers and employees. Many banks are reducing operating hours, restricting lobby access, and temporarily closing branches. Before heading to deposit funds at a bank branch, check the bank's website or call the specific branch to learn of any changes to its operations.

ORS 293.265 and Treasury policy FIN 201 require agencies to deposit moneys within one business day after receipt or collection. Both the statute and our policy authorize agencies to deposit moneys within a reasonable period beyond one business day as long as an agency documents a valid business reason for using a longer period and the period is no longer than necessary to satisfy the business reason. Agencies needing additional time to deposit moneys due to the COVID-19 pandemic should appropriately document the reasons, which could include impacts to agency staffing and impacts to bank branch operations. *See* FIN 201 for more information and a list of items to consider when holding moneys for deposit.

Spear Phishing

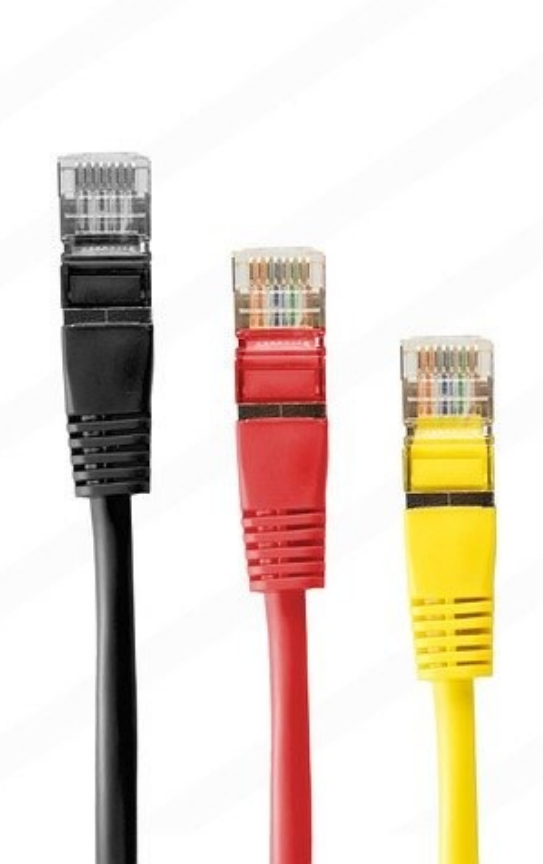
With so many people working from home, and other disruptions, scammers are working to take advantage of the COVID-19 pandemic in a variety of ways. Governments in particular should be aware of increased fraud attempts. All organizations, including state agencies and other governmental entities, must 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.

How to Protect Your Organization

While spear phishing is a sophisticated scam that relies on inside information, there are behaviors and processes that you and your organization can use to avoid becoming a victim.

- Be suspicious of unusual or unsolicited communications.
- Verify communications by contacting individuals or companies at known, trusted phone numbers or e-mail addresses.
- Do not provide information about yourself or your organization except to known, authorized individuals.
- Do not reveal financial or other sensitive information in e-mail.

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.



Accessing Cash Management Systems

Treasury is continuously focused on protecting the state's cash management systems and data. As part of our security framework, we restrict not only *who* can access our systems but also *from where* such authorized users can access our systems. That means agencies must register specific IP addresses that will be used to access our systems. Agencies that have staff working remotely should be mindful of this security requirement and should employ technology solutions, such as VPNs, to ensure that staff are accessing cash management systems from registered IP addresses.

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