

# Fraud Alert



## *Multiple Fraud Alerts in Pacific Northwest*

The Northwest Credit Union Association is receiving information about multiple fraud attempts across the Northwest.

### **HELOC Scams**

The first two fraud attempts both deal with HELOC advances. In each case, an individual will contact a credit union and impersonate a member. The fraudster knows information that only the member should know, but they have somehow obtained the information and can convince the credit union representative that they are the member. Sometimes, the fraudsters will ask for the available credit on the member's HELOC and then request an advance to a checking account while others will call in already knowing the available amount. If a signature is required for the advance, the fraudster can normally produce it without hesitation.

Once the funds are advanced from the HELOC, the fraudster will

retrieve the funds in a few different ways. First, they might ask for a wire transfer. Again, if a signature is required, they are normally able to produce it quickly. The fraudster might also have access to legitimate or counterfeit checks drawn off the member's account. Once the HELOC funds are advanced, the fraudster will write a fraudulent check to access the funds.

It is important to remember that fraudsters are able to access members' signatures via public documents, especially those relating to credit secured by real estate. Not only can the fraudster access the signature, but they can also determine who the creditor is, which leads them to your credit union.

It is important to remember that out-of-wallet questions are a best practice used to help prevent fraud. Asking questions that cannot be found in a credit report or online is one way to help ensure you are talking with your member. It can be difficult to develop questions that cannot be answered by a simple internet search (LinkedIn, Facebook) or having access to the member's credit report. If you are able to center the questions around activity specific to the member's account with the credit union, you have a higher likelihood of determining if you are really talking to your member. Examples of these questions can include when and where the account/membership was opened, information about the other signers on the account, information specific to credit products held

with the credit union, or anything else that is specific to the credit union relationship.

It is also important for credit unions to ensure that any wire transfer security procedures are followed. These procedures could include not accepting a wire transfer request over the phone or fax, having a strong call-back process, supervisor review of all wires, or requiring members to have a specific wire-only password set up with the credit union. Once a wire is sent, it can be very difficult to retrieve the funds if it is later discovered that the wire was not authorized.

### **W-2 Scam**

The IRS recently issued a reminder to businesses regarding a W-2 scam that is common during tax season. This scam usually targets the HR department of a company and includes an urgent request sent via a “spoofed” email from an internal source, usually the CEO or another individual in management. The email will request the W-2 file, a list of employees’ information (including social security numbers), or other payroll related files. The request appears legitimate but is not actually sent from the person supposedly making the request. This could impact credit unions and your members. It is important to have procedures in place for sending/receiving sensitive information, including payroll related records. Credit unions should be aware of this scam and can share

information with their members about the scam by visiting the IRS website: [IRS Warns of W-2 Scam](#).

### **Counterfeit Check Ring**

To round out the fraud alerts, Boise Police Department has alerted financial institutions about a scam involving counterfeit payroll checks. With this particular scam, an out of state crew will travel to a city and steal checks from mailboxes. The crew will then go to a local homeless shelter and hire a local homeless person (or a few) that has a valid picture identification. After hiring someone, the crew will add the homeless person's name to the payee line of the check and drive them around to different financial institutions in order to negotiate as many checks as possible on that account. The person or crew that recruited the homeless individual will never enter the financial institution. If you think that someone at your credit union is attempting to participate in this scam, Boise PD is requesting that the credit union try to obtain the license plate number of the vehicle used to transport the individual cashing the check(s), as long as it is safe to do so. Currently, the two individuals that have been cashing the counterfeit checks in Boise are Kevin Orts and Keith Baker. However, because individuals can easily travel between all major cities in the Pacific Northwest, all credit unions should be aware of this potential scam and contact their local police department if they suspect that the scam is occurring at their credit union.

Fraud and robberies appear to be rapidly increasing in the Pacific Northwest. There are many resources available to help credit unions identify scams, stay aware of robberies, and educate members about safeguarding their information. Your Association has an [Identity Theft Prevention and Response Toolkit](#) available to credit unions to help them educate their members about identity theft. You can also access prior robbery and fraud alerts by visiting our website or contacting the Compliance Department. Additionally, if you would like to report fraud, scams, robbery (actual or attempted), or discuss best practices or training, please don't hesitate to reach out to the Compliance Department at 800.546.4465 or [compliance@nwcua.org](mailto:compliance@nwcua.org).

**Katie Clark CUCE, BSACS**

Regulatory & Compliance Analyst

Northwest Credit Union Association

P: 503.350.2221 | F: 877.928.6397 | 800.995.9064 | [www.nwcua.org](http://www.nwcua.org)

Copyright © 2017 Northwest Credit Union Association  
Idaho Office: 2770 S Vista Ave • Boise, ID 83705  
Oregon Office: 13221 SW 68th Pkwy, Suite 400 • Tigard, OR 97223  
Washington Office: 18000 International Blvd, Suite 350 • SeaTac, WA 98188

**Stop the email clutter:** [customize the types of emails you receive from us.](#)

If you would like to stop receiving **ALL** emails from us, [go here.](#)

Please send any comments about this email to [webmaster@nwcua.org](mailto:webmaster@nwcua.org).

