Northwest Credit Union Association
Idaho • Oregon • Washington

Fraud Alert

Fraud/Scams Hitting the Northwest

Fraudsters have hit the ground running in 2019. We have received several reports of various types of fraud schemes that credit unions need to know about in order to stay vigilant.

Abusing OD/Courtesy Pay privileges: Recently, it has come to the attention of law enforcement in Boise, ID that some individuals are using the available limits offered to members through various courtesy pay programs as a way to gain access to funds that they do not intend to pay back. In one particular case, an individual was instructed to open a new account at any financial institution that would offer courtesy pay right away. The individual was coached to open the new account with $50 and then to immediately withdraw $400-$500 through the courtesy pay feature.

Credit unions should address the risk associated with immediate access to courtesy pay programs and mitigate the risk accordingly. One way to mitigate such risk would be to delay offering the service until the member has a more established relationship with the credit union.

Card Management Apps: Services offered to members to help secure their debit card information can be subject to fraud. Recently, a credit union discovered that fraudsters had obtained payment card information for its members and used that information to register debit card information through its card management app. The app, which allows a member to control their cards (turn them on and off, set usage controls, and receive usage alerts) and receive information regarding purchases, is then being used to gather additional information that the fraudsters utilize to place the cards in a mobile wallet. Even if the transaction is flagged as potential fraud, the fraudster is able to use the information obtained via the app to contact the credit union's card services' fraud department and approve suspect transactions. Additionally, the fraudsters were placing travel alerts on the debit cards through the card services vendor, which disabled fraud detection during the specified period of travel.

The information provided by the impacted credit union indicates that there was a point-of-compromise prior to the time when the cards were added to the management app. The fraudsters needed the cardholder's social security number and the card's PAN, expiration date, and CVN security code in order to utilize the app. In some instances, the e-mail addresses were

suspect and the user information was either a number or a nonsensical series of characters, which indicated potential fraud.

Additionally, the credit union noted that the management app registrations were closely followed by mobile wallet registrations for the same cards. While many of the risk controls for these third party services occur on the vendor side, we recommend that credit unions monitor new registrations for such services to determine legitimacy. Additionally, having controls in place to verify the registration, such as direct member outreach, could help mitigate the risk.

Old Scam, New Trick: We have also heard of a new spin on money mule/online job positing scams. In this case, a member received several deposits through a Peer-to-Peer (p2p) service from various individuals. The member was instructed to say the transfers were from family. The member also deposited a forged check that was from his supposed employer (job posting on Craigslist). The member revealed that the p2p deposits were also from the employer. Additionally, he was instructed to withdraw the cash and purchase bitcoin which was then loaded into a wallet.

In situations like this, it is best to ask questions of your member. For example, if the p2p activity is new, the credit union can inquire about the transactions (as it would with strange check deposits, strange wires, etc.). Additionally, it might help to educate the member regarding p2p activity as most of these service providers prohibit transfers for commercial/retail purposes (which can be an indication of fraud).

Unfortunately, fraud is an ongoing issue for credit unions and their members. With advances in technology, increases in the availability of consumers' personal information, and fraudsters' knowledge of how credit unions operate, credit unions and their members have to be diligent to avoid the losses associated with these scams. Tried-and-true practices still hold firm-- know your members, ask questions, and share helpful information about scams with your members. With the increased role technology plays in facilitating payments, increased oversight is a must.

#CUobsessed

Katie Clark CUCE, BSACS
Director, Regulatory Affairs & Risk Management
Northwest Credit Union Association
503.350.2221 • 800.995.9064 x221
www.nwcua.org