RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type: Awareness | **Watch** | Warning

Combat Mobile Phone Port-Out Scams

Fraudsters are impersonating mobile phone users to have phones transferred to a different carrier – effectively stealing the users' mobile phone number. This is being coined as a port-out scam. Once transferred to a different carrier, the fraudster receives all calls and texts that were intended for the user – including those that can be used to takeover a member's account via online banking. Fraudsters have successfully intercepted one-time passcodes used to authenticate members logging into their account or to initiate transactions within online banking.

Credit unions should educate members on this scam and recommend placing a "port validation password" on their mobile phone account to help prevent having their phone fraudulently transferred to a different carrier.

Details

Mobile phone users switch carriers for a variety of reasons and can carry their phone number with them to the new carrier. Meanwhile, fraudsters are exploiting this capability by impersonating mobile phone users to have the mobile phones ported to a different carrier. The fraudsters harvest the users' personally identifiable information and use this information to impersonate users in having the mobile phones transferred to a different carrier.

A fraudster often ports a user's mobile phone to a different carrier *after* the fraudster has stolen the user's account login credentials. This could increase the risk of account takeovers through online banking for credit unions offering out-of-band authentication, which involves sending a one-time-passcode via text message for login attempts as well as to validate transactions initiated within online banking. Members must enter the one-time-passcode to complete the login or transaction. By transferring a member's mobile phone to a different carrier, the fraudster would receive the one-time-passcode intended for the member.

Using an app-based, rather than text-based, out-of-band authentication solution can help mitigate the risk of account takeovers. In fact, the National Institute of Standards and Technology (NIST) changed its position on sending one-time-passcodes via text message due to its insecurities. In its Special Publication 800-63B (Digital Identity Guidelines), NIST indicated that the use of a secure app-based method of pushing one-time-passcodes is more secure.

Date: April 3, 2018

Risk Category: Scams; Mobile Technology Fraud; Deposit Account Services, Consumer Payments

States: All

Share with:

- ☐ Card Services
- ☐ Electronic Services
- ☐ Executive Management
- ☐ IT
- ☐ Risk Manager

To share risk insights or gain additional assistance:

- Report a RISK Alert
- Ask a Risk Consultant
- Contact a CUNA Mutual Group Risk & Compliance Consultant
  - **800.637.2676**
  - riskconsultant@cunamutual.com

Combat Mobile Phone Port-Out Scam

This scam could also result in fraudulent transactions using credit and debit cards. A fraudster, who has ported a cardholder's mobile phone to a new carrier, could use a counterfeit or stolen credit or debit card belonging to the cardholder to conduct fraudulent transactions. If a card processor's fraud management system detects a suspicious transaction, a fraud analyst could attempt to contact the cardholder to confirm the legitimacy of the transaction by calling the cardholder's mobile phone. However, the call is made to the fraudster who confirms the transaction as legitimate.

Card fraud could be exacerbated when, after confirming the suspicious transaction as legitimate, the card is suppressed for a period of time – usually seven days. It is common practice for card processors to suppress a card when the fraud management system identifies a suspicious transaction that a cardholder confirms as legitimate. When a card is suppressed, transactions on the card are not monitored by the fraud management system.

Many public email service providers offer out-of-band authentication using one-time passcodes that are sent via text message to users' mobile phones. This could easily lead to a compromise of a member's personal email account after a fraudster ports the member's mobile phone to a different carrier.

Major mobile phone carriers, such as T-Mobile and AT&T, are recommending to their customers to place a "port validation password" on their accounts. If a user wishes to port their mobile phone to a different carrier, the new carrier would have to provide the "port validation password" to the existing carrier before the switch can take place.

Risk Mitigation

Credit unions should consider these mitigation tips:

- Alert members of the mobile phone port-out scam.
- Urge members to place a "port validation password" on their mobile carrier account to help prevent their phone from being fraudulently ported to a different carrier.
- Credit unions using or contemplating out-of-authentication using one-time passcodes should consider a secure app-based, rather than text-based, method of transmitting passcodes.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive risk and compliance resources to assist with your loss control. The Protection Resource Center requires a User ID and password.

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for white papers & checklists
- Webinars and Education
- RISK Alerts Library

Check out these areas of practice to help you manage pressing risks.

The Protection Resource Center requires a User ID and Password.

Interested in learning more about emerging risks?
Contact CUNA Mutual Group's Risk & Compliance Solutions at **800.637.2676** or by email at riskconsultant@cunamutual.com for additional risk insights.