RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

SIM Swapping and Port-Out Fraud Leads to Account Takeovers

Fraudsters are hijacking members' mobile devices through SIM (Subscriber Identity Module) swapping and port-out scams that result in account takeovers. Taking control of members' mobile devices allows the fraudsters to intercept online banking two-factor / out-of-band authentication passcodes needed to log in to member accounts.

Details

Fraudsters are hijacking members' mobile devices through SIM swapping and port-out scams that result in account takeovers. Both scams provide the fraudster with the ability to receive calls and SMS text messages intended for the mobile phone users.

- In the **SIM swapping scam**, a fraudster impersonates a mobile phone user and social engineers the user's mobile phone carrier into activating a replacement SIM card the fraudster has in their possession.
- The **port-out scam** is similar except that the fraudster social engineers a mobile phone carrier into porting the user's mobile phone to a different carrier.

These scams are used by fraudsters to intercept two-factor authentication (a.k.a. out-of-band authentication) passcodes that are needed to login to member accounts through online banking. Fraudsters also hack member email accounts and social engineer credit union call center employees to change member mobile phone numbers and/or email addresses to intercept two-factor authentication passcodes.

Consider these fraud cases:

Zelle / P2P Scam: Members respond to a text alert - appearing to come from the credit union - regarding fraudulent debit card transactions. Fraudsters called members responding to the text spoofing the credit union's phone number and claimed to be from the credit union's fraud department.

The fraudsters con members into providing their online banking username which they use with the "forgot password" feature that triggers a two-factor authentication passcode. The fraudsters attempt to con members into providing the passcode, but many refuse. This doesn't stop the fraudsters, however.

They social engineer the members' mobile phone carriers into activating a replacement SIM card which allows the fraudsters to intercept the passcodes. The fraudsters also used other tactics to intercept the passcodes, including social engineering credit union call centers into changing member mobile phone numbers and/or email addresses. They also hacked members' email accounts to intercept the passcodes.

Date: November 2, 2021

Risk Category: Scams; Fraud; Mobile Devices; Account Takeovers

States: All

Share with:

- ☐ Executive Management
- ☐ Member Services / New Accounts
- ☐ Risk Manager
- ☐ Transaction Services

Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.

SIM Swapping and Port-Out Fraud Leads to Account Takeovers

Wire Fraud: A fraudster successfully social engineered a member's mobile phone carrier into activating a replacement SIM card in the fraudster's possession. The fraudster then called the credit union – impersonating the member – and requested a $190,000 wire and successfully answered the security questions.

Prior to performing the callback verification, the credit union employee confirmed that the phone number on the account had not been changed in the last 60 days. The callback was performed but the call went to the fraudster's mobile phone and again successfully answered the security questions.

Cryptocurrency has been one of the primary targets in the SIM swapping scam with fraudsters stealing millions of dollars in cryptocurrency. Cryptocurrency exchanges traditionally require two-factor authentication for users.

Risk Mitigation

Credit unions should consider these loss controls:

- Warn members about these scams. Some warning signs to share include:
  - Friends might tell you that your social media accounts have been hacked and you see the posts you never made.
  - The phone might start behaving strangely. Texting and calling may not work or the phone network will show no signals. In addition, your SIM card will not show your service provider company.
  - If you're on WiFi, you might start getting emails about account changes.
  - Some wireless carrier services use client email to send notifications. For example, if your email account is not compromised yet, you will receive a notification via email. Now you know that your new SIM card got activated even though you never requested a new SIM card.
  - You are no longer the owner of your accounts. It is because your account detail got changed by the attacker.
- Advise members to put a port freeze or PIN or password on their mobile carrier account. This will help prevent a SIM swap and/or porting service to another carrier.
- Some carriers also have features that could potentially stop SIM swapping. For example, Verizon has a feature that can be enabled from their My Verizon app called "Number Lock." This feature enables customers to prevent an unauthorized port out or SIM swap of your mobile number.
- Adopt a more secure form of two-factor authentication, such as a passcode generating token (hard or soft) or push notifications to a dedicated app residing on the member's mobile device.

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 efforts. The Protection Resource Center requires a User ID and password.

- Fraud & Scams eBook
- Two-Factor Authentication Risk Overview
- Social Engineering Fraud Risk Overview
- Member Authentication & Verification Risk Overview
- Peer-to-Peer Payments Risk Overview

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.