TruStage™

RISK Alert

Actionable insights for bond policyholders

Awareness | **Watch** | Warning

Text messages & spoofed websites used to lure members into scam

Fraudulent text messages - appearing to come from the credit union – containing links to spoofed websites are being sent to members. The spoofed websites are made to look like the credit unions' legitimate websites and members are enticed to click on the link and share confidential information such as username, passwords, as well as 2-factor authentication passcodes. These fraud attempts have resulted in losses from account takeovers.

Alert details

SMiShing (SMS text message phishing) is quickly becoming a preferred choice of fraudsters to lure members into giving up their credentials or sensitive information. There have been multiple reports of members receiving fraudulent text messages containing links to spoofed websites made to look like the credit unions' legitimate site.

The text messages have the following themes:

- Member's account has been locked or suspended due to suspicious or fraudulent transactions.
- Unusual/suspicious transactions at Walmart.
- Unusual/suspicious transactions at cryptocurrency exchanges.
- Suspicious Zelle transfer.

Members are instructed to click on the link contained in the message which takes the members to spoofed credit union websites where they are instructed to enter their login credentials – usernames and passwords. The fraudsters immediately use the credentials to login to the member's accounts.

Since the fraudsters used unregistered devices to login to the accounts, a 2-factor authentication passcode is generated and delivered to the member who, in turn, enters the passcode on the spoofed website. The fraudsters immediately use the passcodes to complete the login to the member accounts.

Once logged into the members' accounts, the fraudsters change the member's contact information and then remove funds using Zelle/P2P or ACH transfers.

In other instances, the fraudster calls or texts the member in which they claim to be from the credit union and need the one-time passcode.

The primary institutions that have been used to move funds to have included Metabank; Green Dot; Bancorp Bank; or Coastal Community Bank. However, there may be more financial institutions being used.

Date:
June 20, 2023

Risk category:
Fraud; Scams; SMiShing; Funds transfer; Wire transfer; ACH fraud; Account takeover; Mobile banking

States:
All

Share with:

- Executive management
- IT
- Member services/new accounts
- Risk manager
- Transaction services
- Web development

Facing risk challenges?:
Schedule a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

Risk mitigation

Credit unions should consider these risk mitigation tips:

- Utilize vendors that can assist in detecting and/or taking down spoofed websites. A best practice is to keep a list of these vendors readily available.
- Register all versions of your domain name.
- Require members to actively enroll in P2P or ACH services in person at a branch or through the call center but only after the members are properly authenticated.
- Consider writing a rule requiring lower transfer limits for new payees or new tokens for ACH and Zelle/P2P transfers, respectively.
- Share risk mitigation tips with your members such as:
  - Don't reply to suspicious text messages and refrain from calling the number
  - Don't click on links or open attachments contained in suspicious text messages and emails
  - Report suspicious credit union-themed text messages and emails to the credit union

Risk prevention resources:

Access the **Business Protection Resource Center** for exclusive risk and compliance resources (user ID and password required).

Access the RISK Alerts Library and enter key words in the search feature.

Review these resources:

- Fraud & scams eBook
- The rise of social engineering fraud

For additional support, call 800.637.2676 or email riskconsultant@trustage.com