CUNA MUTUAL GROUP
INSURANCE • SERVICES • ASSET MANAGEMENT

Tools and Resources

CU Members Victimized in Smishing Attacks

July 20, 2011

Summary

In the last few days, credit unions from around the country have reported their members are receiving bogus text message (smishing) alerts. The text message indicates it is from Credit Union Services and advises the member to call the number provided in the text message to have their card reactivated. This is a scam as no credit union would ever ask a member for this type of information using text messaging.

Risk Type:	Account Fraud, Plastic Card Fraud, Scams
State(s):	All States
Related Product:	Bond

Risk Mitigation Recommendations

Details:

In the last few days, credit unions from around the country have reported their members are receiving bogus text message (smishing) alerts. The text message indicates it is from Credit Union Services and advises the member to call the number provided in the text message to have their card reactivated. This is a scam as no credit union would ever ask a member for this type of information using text messaging.

Credit unions have reported multiple phone numbers provided in text messages sent to credit union members to call to have their card reactivated. One credit union reported that some of their members responded to the text and provided the requested card information.

Because of the increase in both smishing (text message phishing) and vishing (phone call phishing) attempts directed towards members asking for personal or financial information, credit unions should continue to educate the members to never respond to this type of request. If your members provide their card information to the fraudster, the impacted cards should be blocked immediately to help prevent potential card fraud.

Risk Mitigation Recommendations:

Credit unions should continue their efforts in creating member awareness of social engineering tactics, such as smishing and vishing, used by fraudsters to obtain personal and/or financial information. Continue to educate members to never respond to any type of request for personal or financial information being requested by text, phone or email. This can be accomplished by posting an alert message on the credit union's phone system, website and newsletters.

If the credit union is able to capture the telephone number used by the fraudster, report the number to the following organizations:

- The Federal Trade Commission at spam@uce.gov.
- The member's landline or mobile phone carrier.
- The credit union's local telephone carrier.

Related Resources:

- Protection Resource Center for additional RISK Alerts (id/password required)
  - Phishers Focus on Text Messaging and Phone Calls