

Please be aware a fraudulent text message was sent to many Mississippi consumers this weekend from a party falsely representing itself as the Mississippi Credit Union Association. We posted a fraud alert and additional details on [www.msCUA.com](http://www.msCUA.com) yesterday morning.

Although this type of “phishing” scam is not new, it is, unfortunately, becoming more frequent. Both bank and credit union names have been used in previous scams of this type. The names of several credit unions in Mississippi have already been “hijacked” this year for use in text message fraud. (Phishing via phone call is also on the rise. [Read more here.](#))

#### **How does a phishing scam work?**

Messages from a party falsely representing itself as a financial institution, such as a bank or credit union, are sent to consumers at random. (In fact, you may not even have an account with the bank or credit union whose name is “hijacked” and used in the scam.) The message typically states there is a “problem” with an account/card or an account/card requires “verification,” “re-activation” or “unlocking.” Those that respond to the message are asked to enter/provide account and PIN numbers. Those that do provide the personal financial details the message requests may become the victim of fraud.

#### **How did they get my phone number?**

The message is likely distributed at random. A computer may be used to generate a list of numbers that could be possible for a certain geographic area, based on area code or prefix. The computer simply calls or sends a message to that randomly generated list of numbers.

(It is important to reassure members that these types of attacks are not generally the result of any type of information “breach” at their credit union or bank. Receiving this type of scam message does not mean a crook HAS their information -- It means they **WANT** their information. They are trying to fool the consumer into giving it to them.)

#### **I responded to the message and provided personal information. What do I do now?**

Act immediately if you've been hooked by a phisher. If you provided account numbers, PINS, or passwords to a phisher, notify the companies with whom you have the accounts **right away** and tell them you may be a victim of fraud. They can help you close compromised accounts and establish account fraud alerts.

For information about how to put a “fraud alert” on your files at the credit reporting bureaus and other advice for ID theft victims, visit the Federal Trade Commission’s ID Theft site: <http://www.ftc.gov/bcp/edu/microsites/idtheft> or call 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

#### **I didn't respond to the message, but I believe it is fraudulent. What do I do now?**

Report the message to the company that the phisher was impersonating. However, do not use any contact information that was provided in the message; Instead, look up the company’s official phone number in the phone book or find their official website.

#### **Should I report it to the police, Better Business Bureau or others too?**

You certainly may. However, there is little authorities can do about this type of fraud. The criminals that set-up the fraudulent phone numbers, website addresses or email addresses used in the messages move very quickly. In most cases, the numbers or websites related to the scam message have already been removed long before authorities can even be notified.

There is also, unfortunately, little that the authorities, phone companies or the company whose name is used in a phishing message can do to **prevent** the message from being distributed. Therefore, the best protection against becoming a victim of fraud is knowledge: *Do not respond to unsolicited text messages, phone calls or emails requesting personal information. Ever.*

#### **How do I know if message, phone call or email may be an attempt at fraud?**

Unsolicited contact requesting you to enter or disclose account or personal information is almost always an attempt at fraud. Legitimate companies simply do not conduct business that way.

Fraudsters try to create a sense of urgency and need for “immediate” action. The “hook” may come in many forms:

- Account Activation, or De-activation
- Confirming Account or Credit Card Numbers
- Account Status Alert

- Changes to Terms and Conditions
- Irregular Activity

Here are some examples of phishing scam messages:

- “Your Federal Credit Union card has been deactivated. To reactivate please visit urgent **Error! Hyperlink reference not valid.** address removed] or call (555) 555-5555.”
- [8665555555@abccreditunion.com](mailto:8665555555@abccreditunion.com) ABC Credit Union. Your account has been locked. Call online banking service @ 866-555-5555 for assistance”
- “There has been irregular activity in your account. Please call XYZ Bank customer service at (555) 555-5555 or go to **Error! Hyperlink reference not valid.** address removed]”
- [8775555555@xyzcreditunion.com](mailto:8775555555@xyzcreditunion.com) Customer issue. ABC Credit Union service frozen. Please call 877-555-5555”

**Bottom line: NEVER respond to unsolicited phone call, text message or email requesting account or other personal information. If you have doubts about the legitimacy of the request, contact the company directly through a trusted phone number or website (do not use the contact information provided in the request).**