

**CONSUMER ALERT:****BEWARE OF FINANCIAL SCAMS VIA TEXT MESSAGE, PHONE OR EMAIL**

Most consumers have heard of what used to be a mainly email-distributed type of fraud known as “phishing.” But did you know criminals are now using text messages and phone calls for phishing scams? Use the information below to help avoid becoming a victim of financial fraud.

***HOW A PHISHING SCAM WORKS:***

- 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” for the scam.)
- The message typically states there is a “problem” with an account/card or an account/card requires “verification,” “re-activation” or “unlocking.” The message wording usually tries to create a sense of urgency, making the receiver feel like if they don’t act now, they won’t be able to access their money.
- Those that respond by following the directions in the message are routed to a person, website or automated answering service that asks them to enter/provide account and PIN numbers.
- Those that 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 may be possible for a 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 note that these types of attacks are not generally the result of your information having already been obtained or stolen. Receiving this type of scam message does not mean a

crook HAS your information. It means they **WANT** your information. They are trying to fool you in to giving it to them. That's why they call it "phishing," crooks are throwing out a line to see who they can catch.

***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 CALLED THE NUMBER IN THE MESSAGE, BUT I DIDN'T ENTER OR PROVIDE ANY PERSONAL OR ACCOUNT INFORMATION. AM I AT RISK?***

If you called the number, **but did not enter or disclose any account or personal information**, it is not likely you are at risk.

***I DIDN'T RESPOND TO THE MESSAGE AT ALL, BUT I DO BELIEVE IT IS FRAUDULENT. WHAT SHOULD I DO?***

If you like, you can 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. You may find the scam has already been reported to the company, but it never hurts to make sure they are aware.

***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 crooks that set-up the fraudulent phone numbers, website addresses or email addresses used in the messages move very quickly and are difficult to track and catch.

### ***CAN THESE SCAMS BE STOPPED?***

Unfortunately, there is 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.

The best protection against becoming a victim of fraud is knowledge: **Do not respond to unsolicited text messages, phone calls or emails requesting account numbers and PIN/passwords.** Ever. If you are afraid something may be wrong with your account, contact your financial institution directly at a trusted phone number and make an inquiry.

(Note: Many of these scams are conducted on Saturday & Sunday. Why? Because many financial institutions aren't open on weekends and fraudsters know consumers won't be able to make contact to verify if the message is authentic. That gives the fraudsters more time to conduct their scam.)

### ***HOW DO I KNOW IF A MESSAGE, PHONE CALL OR EMAIL MAY BE AN ATTEMPT AT FRAUD?***

Unsolicited contact (meaning you didn't initiate the contact) requesting you to enter or disclose an account number and PIN/password is almost always an attempt at fraud. Although legitimate companies you have accounts with may contact you, they typically ask you to answer pre-arranged security questions or provide partial (like the last four digits) account or personal numbers to verify you are the account holder when speaking with you. **They do not ask you to disclose your account PIN or password.** Anyone that does so is likely trying to gain access to your account for the purpose of committing fraud.

Fraudsters try to scare you by creating 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 [http://\[fraudulent address removed\]](http://[fraudulent address removed]) or call (555) 555-5555.
- 866555555@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 [http://\[fraudulent address removed\]](http://[fraudulent address removed])
- 8775555555@abcbank.com Customer issue. ABC Bank service frozen. Please call 877-555-5555
- A phone call phishing scam would be similar. It may be an automated message or a “real” person reporting “account problems” similar to those in the text messages and ultimately asking for your account number and PIN/password.

**Bottom line: NEVER respond to an unsolicited phone call, text message or email requesting an account number and PIN/password. 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 message/request).**

Additional tips and advice on avoiding phishing fraud and other scams can be found on The National Consumer League's National Fraud Information Center: <http://www.fraud.org>.