FRAUD ALERT

Date: June 18, 2012
Subject: AT&T/Credit Union SMishing Scam

Common Scams

Phishing: Phishing is when internet fraudsters impersonate a business in an attempt to trick you into giving out your personal information, such as usernames, passwords, and credit card details. Legitimate businesses don't ask you to send sensitive information through insecure channels.

Example:

> For example, a fraudulent email may state that a federal credit union needs to update your account information and will request that you click a link in the email. The link embedded in the message directs members to a counterfeit version of credit union's website with an illicit form that solicits account numbers and confidential personal information.

For more information, visit:

- **FTC's Phishing E-card**
  www.ftc.gov/bcp/edu/multimedia/ecards/phishing/index.html
- **FTC's Consumer Alert on Phishing**
  www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm.
- **OnGuardOnline.gov**
  www.OnGuardOnline.gov/phishing. OnGuardOnline.gov is the federal government's website to help you be safe, secure and responsible online.

SMishing: The term SMishing is a combination of "SMS" and phishing. SMishing uses cell phone text messages or SMS (Short Message Service) to deliver a message in order to get you to divulge your personal and financial information. The method used to obtain information in the text message may be a web site URL, however it has become more common to see a phone number that connects to an automated voice response system.

Unsolicited Text Messages: Unsolicited text messages sent to cell phones urge the recipient to call a number provided for information about account discrepancies and then solicits individual account information and pin numbers. Cell phone users should

be wary of unsolicited text messages. Such messages should be deleted and all deleted text messages should be removed, if possible, as the perpetrators have been known to use Spyware1 in conjunction with their text message solicitation.

Vishing: The term vishing is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations, are known to the telephone company, and are associated with a bill-payer. The victim is often unaware that voice over Internet Protocol (VoIP) allows for caller ID spoofing thus providing anonymity for the criminal caller. Rather than provide any information, the consumer should contact their financial institution or credit card company directly to verify the validity of the message using contact information they already have in their possession (i.e. do not use contact information provided in the suspicious message).

A spamming and phishing scam was reported by AT&T that involves AT&T prepaid cell phones. The spamming from the prepaid cell phones solicits credit union customers to call a number that attempts to obtain account information.

The SMS phishing or “SMishing” has occurred since January 2011. AT&T has cancelled hundreds of these prepaid accounts due to fraud. AT&T has developed a few leads and continues to investigate this matter. If you have received a SMS phishing text, it is advised that you do not respond. These texts are an attempt to steal a consumer’s identity.

1. Consumers who suspect that they have been a victim of SMS phishing are advised to contact the fraud department of each of the following three major credit bureaus and report that their identities have been stolen. They should also consider placing a "fraud alert" on their files and request that no new credit be granted without prior approval.

	Equifax	Experian	Trans Union
Address	P.O. Box 740241 Atlanta, GA 30374	P.O. Box 2104 Allen, TX 75013	P.O. Box 6790 Fullerton, CA 92634
Web Address	www.equifax.com	www.experian.com	www.transunion.com
Order Credit Report	1-800-685-1111	1-888-EXPERIAN (397-3742)	1-800-916-8800
Report Fraud	1-800-525-6285	1-888-EXPERIAN	1-800-680-7289

		(397-3742)	

2. For any accounts that have been fraudulently accessed or opened, the customers should contact the security department of each affected creditor or financial institution. The customers should consider closing these accounts. On any new accounts the customers open, they should consider using a password, but not their mothers' maiden names.

3. The customers should file a report with their local police department or the police where the identity theft took place, if known. They should retain a copy of the police report in the event that their bank, credit card company or others need proof of the crime at a later date.

For additional information, please contact the NCUA Consumer Assistance Center at 1-800-755-1030.