



For Immediate Release
August 1, 2008

District Attorney Nola Foulston warns of a scam involving telephone calls to consumers between approximately 9:00 pm. yesterday and as late as 10:30 a.m. this morning or after. The calls are allegedly placed by a local bank. The recording states, "This is an automated call from ___ Bank. We are sorry we had to lock your bank account access. In order for you to activate your account, please call 319.985.1447."

Those consumers who have caller I.D. report that the telephone number appearing on their I.D. is in fact the number of the local bank purportedly making the call. However, the number the customer is asked to call to re-activate their account does not belong to the local bank.

Clearly the number of the Bank has been "spoofed" to appear on one's telephone I.D.

The Bank has reported this to the FBI, the Secret Service and the local Police Department as this message is not being made by the Bank or with its approval or consent. The Bank, in this instance, is also a victim, just like the individuals who receive the recorded telephone message. Many of the individuals receiving the calls are not even customers of the local bank.

THE RECORDED MESSAGE IS NOT TRUE AND IS A SCAM.

In the event you receive such a telephone call, do **not provide the information.** It is all a scam to get your personal information so the caller can obtain monies from your account without your permission. Never give out personal information over the phone to someone who places a call to you. **Financial institutions do not solicit customer account or credit card information from their customers.**

If you receive a request for information you believe may be legitimate, contact your financial institution before filling out forms or providing information. Often the financial institutions who are the subject of such attacks have warnings posted on their websites outlining the known scams and providing details about the various techniques.

Nola Foulston advises consumers of the following in order to avoid scam artists who try to trick people into giving out personal financial information:

- 1. Never give out bank account or credit card numbers over the phone if you did not initiate the call to a reputable, known business.**

2. **DO contact YOUR bank to find out if they have seen any type of unwanted activity with your account;**
3. **DO get on YOUR bank's official website, find out the number for its Fraud and/or Security Department and speak with them regarding the validity of the telephone calls or e-mail(s) received.**

In the event you provided sensitive information before you realized the telephone call or an e-mail was phony, we suggest you take the following steps:

- 1) Contact YOUR bank, alert them on what occurred and request help on securing your accounts/money;**
- 2) Contact the three main Credit Bureaus and place fraud alerts on you account(s) to safeguard against any future fraudulent credit activity;**
- 3) Report the incident to the local law enforcement agency and obtain the incident number assigned to your call;**
- 4) Maintain a file of all future incidents regarding your personal information that may arise from this incident. Keep records of all names, addresses, phone numbers of the people you speak to, keep records of the times you spoke with them and a summation of the conversation(s). All this information may be important if action is required by you later.**

If you think you have been a victim of a scam, please call the District Attorney's Office at 316-660-3653.

For additional information on protecting yourself from these crimes, contact the Consumer Fraud and Economic Crimes Division of the District Attorney's Office at 660-3600 or go to the District Attorney's website at <http://sedgwickcounty.org/da> for helpful links.

*District Attorney Nola Tedesco Foulston
18th Judicial District of Kansas*