NEWS RELEASE

For Immediate Release – November 15, 2012

Contact: Kristin Ewing
405/424-5252 or kristin@oba.com

Phone scam striking Oklahoma

OKLAHOMA CITY — Oklahomans are now receiving phone calls from people claiming to be with Microsoft or other technical support companies regarding their computer safety. Intending to protect their computer, consumers are granting remote access to the person on the other end of the phone. Unfortunately, the person on the other end of the call is a cyber fraudster. Instead of improving computer safety, fraudsters are able to steal data resulting in account takeovers through the remote access.

Microsoft will never call a consumer directly to notify you of issues. According to Microsoft, cyber criminals will work to:

- Trick you into installing malicious software that could capture sensitive data, such as online banking user names and passwords. They might also then charge you to remove this software;
- Take control of your computer remotely and adjust your settings to leave your computer vulnerable;
- Request credit card information so they can bill you for phony services;
- Direct you to fraudulent websites and ask you to enter credit card and other personal or financial information;
- Convince you your Windows Operating System has been corrupted and will fail.

Microsoft suggestions if someone calls claiming to be from Microsoft tech support include:

- Do not purchase any software or services;
- Ask if there is a fee of subscription associated with the "service." If there is, hang up;
- Never give control of your computer to a third party unless you can confirm that is a legitimate representative of a computer support team with whom you are already a customer;
- Take the caller's information down and immediately report it to your local authorities;
- Never provide your credit card or financial information to someone claiming to be from Microsoft tech support.

-- MORE --

If you have fallen prey to this scam, you should notify your bank if you have shared remote access that would have left you vulnerable to cyber thieves stealing this data. If you have any doubt about whether they may have installed malicious software on your computer, you should take it to a reputable computer repair shop where it can be easily removed, then be alert for changes to your bank account or credit card statements.

This scam has been reported in the USA and numerous other countries. Authorities have been learning that the fraud operations have been based largely in India. Despite arrests by American, Australian and Canadian authorities, the scam continues to be ongoing and increasing in volume. Oklahoma bankers continue to educate and partner with their customers to keep their money safe as the cyber environment becomes more challenging.

The OBA conducts more than 70 educational programs and seminars each year, which reach more than 5,000 bankers across the state. The Association represents approximately 230 banks across the state and serves as the primary advocate for the banking industry. It's also heavily involved in fraud training and prevention as well as legal and compliance services and communications for its member banks.

# # #