NEWS RELEASE

For Immediate Release – October 22, 2013

Contact: Kristin Ewing
405/424-5252 (W)
630/815-9085 (C)
kristin@oba.com

**** This is the fourth of four releases about cyber security. Releases will be distributed on Tuesdays in October.*

Oklahoma banks offer tips for protecting yourself online

October is National Cyber Security Awareness Month

OKLAHOMA CITY — The Internet is a powerful resource that many Americans have come to depend on for everyday activities like shopping, banking and connecting with friends. Yet for all the advantages the Internet has, it can also make users vulnerable to fraud, identity theft and other scams. According to a Norton Cybercrime Report, 556 million adults worldwide were victims of cybercrime in 2012.

"As cybercrime becomes more prevalent, it is important for users to take steps to protect themselves online," said Elaine Dodd, OBA vice president – fraud. "Safeguarding your personal information and money is a partnership between you and your bank. Oklahoma community banks work diligently to protect your information and so should you."

In recognition of National Cyber Security Awareness Month, Oklahoma community banks, in partnership with the Oklahoma Bankers Association, offer the following tips to help consumers stay safe and secure online:

- **Keep your computers and mobile devices up-to-date.** Having the latest security software, web browser and operating system are your best defenses against viruses, malware and other online threats. Turn on automatic updates so you receive the newest fixes as they become available;
- **Set strong passwords.** A strong password is at least eight characters in length and includes a mix of upper and lowercase letters, numbers and special characters;
- **Watch out for phishing scams.** Phishing scams use fraudulent emails and websites to trick users into disclosing private account or login information. Do not click on links or open any attachments or pop-up screens from sources you are not familiar with. Forward phishing

emails to the Federal Trade Commission (FTC) at spam@uce.gov and to the company, bank or organization impersonated in the email;

- **Keep personal information personal.** Hackers can use social media profiles to figure out your passwords and answer those security questions in the password reset tools. Lock down your privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of requests to connect from people you do not know;
- **Secure your internet connection.** Always protect your home wireless network with a password. When connecting to a public Wi-Fi network, be cautious about what information you are sending over it;
- **Shop safely.** Before shopping online, make sure the website uses secure technology. When you are at the checkout screen, verify that the web address begins with *https*. Also, check to see if a tiny locked padlock symbol appears on the page; and
- **Read the site's privacy policies.** Though long and complex, privacy policies tell you how the site protects the personal information it collects.

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.

# # #