NEWS RELEASE

For Immediate Release – October 14, 2014

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

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

Protect yourself online with tips from Oklahoma banks

October is National Cyber Security Awareness Month

OKLAHOMA CITY — With 12 victims per second, there were 378 million victims of cybercrime worldwide in 2013 according to the Norton Cybercrime Report. With the ease and convenience of the Internet, it is easy for Americans to let their guard down. In the past year, 50 percent of online adults have been victims of cybercrime including fraud, identity theft and other scams.

"When we're using the Internet at home or work, we feel pretty secure in our safety and that sense of security can easily flow over to using the Internet elsewhere," said Elaine Dodd, OBA vice president – fraud. "But truly, it doesn't matter where you are, you need to take precaution at all times to safeguard your personal information and money. Our community banks here in Oklahoma work diligently to help you protect your identity and information but you need to as well."

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:

- **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;
- **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;
- **Keep personal information personal.** Hackers can use social media profiles to figure out your passwords and answer the security questions when resetting a password. Lock down your

privacy settings and avoid posting things like birthdays, addresses, mother's maiden name, etc. Be wary of any requests to connect from people you do not know;

- **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 at spam@uce.gov and to the company, bank or organization impersonated in the email;
- **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 polices 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.

# # #