NEWS RELEASE

For Immediate Release – October 8, 2013

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

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

Oklahoma bankers offer tips to small businesses for combating fraud

October is National Cyber Security Awareness Month

OKLAHOMA CITY — Cybercriminals are targeting small businesses with increasingly sophisticated attacks. Criminals are using spoofed emails, malicious software and online social networks to obtain login credentials to businesses' accounts, transfer funds from the accounts and steal private information, a fraud referred to as "corporate account takeover."

"Small businesses remain in the crosshairs of cybercriminals," said Elaine Dodd, OBA vice president – fraud. "You can shield your company from an attack through a strong partnership with your financial institution."

Combating account takeover is a shared responsibility between businesses and financial institutions. Bankers can explain the safeguards small businesses need and the numerous programs available that help ensure fund transfers, payroll requests and withdrawals are legitimate and accurate. Companies should train employees about safe Internet use and the warning signs of this fraud because they are the first line of defense.

"We're far more effective at combating account takeover when we combine resources than going at it alone. Bankers can teach you about the tools your business can use to minimize this threat," Dodd said.

As part of National Cyber Security Awareness Month, the community banks of Oklahoma, in partnership with the Oklahoma Bankers Association, offer small businesses the following tips to help prevent account takeover:

- **Protect your online environment.** It is important to protect your cyber environment just as you would your physical location. Do not use unprotected internet connections. Encrypt sensitive data and keep updated anti-virus and anti-spyware protection on your computers. Change passwords from the default to something complex, including at point-of-sale terminals;

- **Partner with your bank for payment authentication.** Talk to your banker about services that offer call backs, device authentication, multi-person approval processes, batch limits and other tools that help protect you from unauthorized transactions;
- **Pay attention to suspicious activity and react quickly.** Put your employees on alert. Look out for strange network activity, do not open suspicious emails and never share account information. If you suspect a problem, disconnect the compromised computer from your network and contact your banker. Keep records of what happened; and
- **Understand your responsibilities and liabilities.** The account agreement with your financial institution will detail what commercially reasonable security measures are required in your business. It is critical that you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a takeover. Talk to your banker if you have any questions about your responsibilities.

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.

# # #