



OKLAHOMA
BANKERS
ASSOCIATION

NEWS RELEASE

For Immediate Release – October 21, 2014

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

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

Guidance from Oklahoma bankers to help small businesses combat fraud

October is National Cyber Security Awareness Month

OKLAHOMA CITY — Small businesses are a target for cybercriminals using increasingly sophisticated methods to attack. Spoofed emails, malicious software and online social networks are used by cybercriminals to obtain login credentials to businesses' accounts, transfer funds from the accounts and steal private information, which is commonly referred to as a "corporate account takeover."

"Cybercriminals don't really care about the size of their target," said Elaine Dodd, OBA vice president – fraud. "All they care about is they were successful. Perception is that a smaller business would be more susceptible to an attack. Small businesses in Oklahoma can shield their company from an attack though with a strong partnership with their financial institution."

It is a shared responsibility between businesses and financial institutions to combat corporate account takeovers. Banks 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 fraud because they are the first line of defense.

"When we combine resources instead of going at it alone, we're far more effective at combating corporate account takeovers. Our Oklahoma bankers can teach business owners about the tools they can use to minimize these threats." Dodd said.

In recognition of National Cyber Security Awareness Month, Oklahoma community banks, in partnership with the Oklahoma Bankers Association, offer small businesses the following tips to help prevent corporate account takeovers:

- **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 IT provider and banker. Keep records of what happened;
- **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 you understand and implement the security safeguards in the agreement. If you don't, you could be liable for losses resulting from a corporate account 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.

###