



OKLAHOMA
BANKERS
ASSOCIATION

NEWS RELEASE

For Immediate Release – January 27, 2015

Contact: Kristin Ewing, APR

405/424-5252 (W)

630/815-9085 (C)

kristin@oba.com

Simple steps to stop a cyber-thief

OKLAHOMA CITY — In recognition of National Data Privacy Day on Jan. 28, Oklahoma community banks are urging customers to take an active role in protecting their data.

“Protecting Oklahomans and their money and information is the top priority for all Oklahoma banks,” said Elaine Dodd, vice president – fraud at the Oklahoma Bankers Association. “Our banks are work diligently to protect their customers but it is important for Oklahomans to do what they can to keep their information safe.”

Oklahoma community banks in partnership with the Oklahoma Bankers Association suggest following these four tips to help ensure the safety of personal information:

1. **Create c0mplic@t3d passwords.** Avoid birthdays, pet names and simple passwords such as 12345 and incorrect. It is also important to change passwords at least three times a year. Because friendly theft – theft by someone the victim knows – is the most common type of identity theft or fraud, don’t share your passwords with family members or friends and be mindful of who has access to your personal information. Also, make sure you don’t use the same password for every account;
2. **Keep tabs on your accounts.** Check account activity and online statements often, instead of waiting for the monthly statement. You are the first line of defense because you know right away if a transaction is fraudulent. If you notice unusual or unauthorized activity, notify your bank right away. When a customer reports an unauthorized transaction in a timely manner, the bank will cover the loss and take measures to protect the account;
3. **Stay alert online.** Be sure computers and mobile devices are equipped with up-to-date anti-virus and malware protection. Never give out your personal financial information in response to an unsolicited email, no matter how official it may seem. Your bank will never contract you by email asking for your password, PIN or account information. Only open links and attachments

from trusted sources. When submitting financial information on a website, look for the padlock or key icon at the top of bottom of your browser and make sure the Internet address begins with “https.” This signals that your information is secure during the transmission; and

4. **Mobilize your defenses.** Use the passcode lock on your smartphone, tablet and other devices. This will make it more difficult for thieves to access your information if your device is lost or stolen. Before you donate, sell or trade your mobile device, be sure to wipe it clean using specialized software or using the manufacturer’s recommended technique. Some software allows you to wipe your device remotely if it is lost or stolen. Use caution when downloading apps as they may contain malware and avoid opening links and attachments – especially from senders you don’t know.

If you find yourself a victim of fraud and suspect your personal information has been compromised, you should take the following steps:

- Call your bank and credit card issuers immediately so they can take necessary steps to protect your account;
- File a police report and call the fraud unit of the three credit reporting companies;
- Consider placing a victim statement in your credit report and a fraud alert on your account;
- Keep a log of all the contacts you make with authorities regarding the matter. Write down names, titles and phone numbers in case you need to contact them again or refer to them in future correspondence; and
- Contact the FTC’s ID Theft Consumer Response Center at 1-877-ID-THEFT (1-877-438-4338) or www.ftc.gov/idtheft.

Data Privacy Day commemorates the 1981 signing of the first legally binding international treaty dealing with privacy and data protection. It is led by the National Cyber Security Alliance, a non-profit public private partnership focused on cyber security education for all online citizens.

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.

###