Ambler Savings Bank and ICBA Encourage Consumers to Protect their Data

Ambler, PA (November 2015) – Americans live in a mobile society, relying on smartphones, tablets and computers to gather news, make purchases, interact with friends and family, and connect with financial institutions. Increasingly, cybercriminals compromise the networks that support these devices. This often results in identity theft, which can also yield financial losses and safety for consumers. In fact, a recent report from the Center for Strategic and International Studies (CSIS) found that computer hackers have stolen the personal information of approximately 40 million U.S. residents.

The Independent Community Bankers of America® (ICBA) and Ambler Savings Bank are offering tips to help consumers avoid having their online financial information disrupted or stolen. ICBA, along with more than 6,000 community banks across the country, urge consumers to remain vigilant and protect themselves from potential credit card and bank fraud.

ICBA and Ambler Savings Bank offer the following tips to help consumers safeguard their online accounts:

- When sending sensitive information via the Internet, make sure "https:" appears in the address bar. This means the information you are transmitting is encrypted.
- Ensure the wireless network you use is password-protected, and choose a strong password and update it frequently for your work and home wireless networks. Likewise, always use a passcode on your mobile phone or tablet to stop an unauthorized user from accessing your device.
- Don't enter sensitive information into your phone when others can see what you're entering.
- Set the privacy settings on frequented social network sites. Cybercriminals often learn about people and their families and friends via social media in an attempt to spoof or phish you and your network.
- Remain cautious of someone who isn't who they say they are or if the name and area don't match what appears on caller ID. This is often how spoofing occurs.
- Never respond to text messages, emails or phone calls from companies alleging to be your bank, government officials or business representatives that request your banking ID, account numbers, user name or password.
- Similarly, don't click on links sent to you from unknown sources via text message because they are likely malware.
- Beware of "get rich quick" schemes; never voluntarily give out your bank account information or security credentials.

You can learn more about cyber and data security by visiting the Stay Safe Online website. Online resources for community banks regarding cyber and data security are available on ICBA's Data Breach Toolkit.