Jersey State Bank Raises Awareness for Data Privacy Day Jan. 28

In recognition of National Data Privacy Day on January 28th, 2015, Jersey State Bank is urging customers to take an active role in protecting their data. "Jersey State Bank's first priority is to protect our customers' money and information," said Jenny King, IT Officer. "We use a combination of safeguards to protect our customers' information, and we encourage our customers to partner with us in that effort."

To help ensure the safety of personal information, Jersey State Bank suggests following these four tips:

1. **Create c0mplic@t3d passwords.** Avoid birthdays, pet names and simple passwords like 12345. 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 and be mindful of who has access to your personal information.

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 contact 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 or bottom of your browser, and make sure the Internet address begins with "https." This signals that your information is secure during transmission.

4.   **Mobilize your defenses.** Use the passcode lock on your smartphone 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 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.

Tips for Victims:

If you are 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 re-contact them or refer to them in future correspondence.
- 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.

Jersey State Bank, the only locally owned Bank in Jersey County, has a long history of providing financial products and services to Jersey County and the surrounding area. Established in 1903, the Bank has assets in excess of $150 million and currently two offices to serve its customers in Jerseyville and Grafton.