**Identity theft tips**

Do not give out personal or financial information on the phone, through the mail or over the internet unless you’ve initiated the contact or know who you are dealing with.

Maintain your computer with virus and malware protection and regular security updates.

Do not click on links or attachments in unsolicited e-mail or texts. It’s easy for fraudsters to copy corporate or government logos into fake e-mails that can install malware on your computer.

For security purposes do not use unsecure public Wi-Fi for personal transactions.

Use strong passwords you can remember. Choose combinations of upper and lower-case letters, numbers and symbols that are hard for a hacker to guess.

Take precautions on social networking sites. Criminals go there to gather details about you to figure out and reset your passwords.

Always log off when you are done.

Close the Internet Browser when finished and/or reopen a new one between sites to help break cookie connections from each site.

Don’t use common names as a password.

When making a purchase, look for the “https” and the padlock. The “s” stands for secure.

Monitor your accounts regularly and report suspicious activity.

Notify Valley Premier Bank before traveling. This will help ensure that legitimate purchases are approved. Just let us know when and where you will be traveling.

Review each of your three credit reports annually. Visit www.annualcreditreport.com or call 877-322-8228.

Shred documents with personal and financial information.

Limit what you carry. When you go out, only take the identification and credit or debit cards you need. Leave your Social Security card safe at home.

Take outgoing mail to the post office collection box or post office. Promptly remove mail from your mailbox. If you will be away for a few days, request a vacation hold.