Important Information About Identity Theft

You work hard for your money. We work hard to protect it. Arm yourself with knowledge about identity theft, and together, we can do even more to put the bad guys out of business. From fraudulent phone calls to deceptive e-mails, identity theft appears in many shapes and sizes. That's why Regions Bank combines intensive employee training with state-of-the-art computer technology to protect both our customers' finances – and their privacy. Here are some useful tips to follow in order to lessen your chances of becoming a victim:

Identity Theft

- Never give out your Social Security number or your account numbers over the telephone unless you initiated the call.
- Tear up receipts, bank statements or unused credit card offers before you throw them away.
- Protect your personal identification numbers and passwords; change them frequently. Never carry this information with you.
- Photocopy the contents of your wallet.
- If your wallet is lost or stolen, contact the fraud department of any one of the three national credit reporting agencies – Equifax (1-800-685-1111), Experian (1-888-397-3742) and/or TransUnion (1-800-680-7289) – to place a fraud alert on your credit file.
- Contact the Social Security Administration (1-800-772-1213) to report someone fraudulently using your Social Security number.
- File a police report in the jurisdiction where your wallet disappeared. Get a copy of the report to submit to creditors and others who may require proof of the crime.
- Review your account statements, and immediately report any inaccuracies or unauthorized charges.
- Do not e-mail confidential information to the bank using your personal e-mail accounts. You may e-mail Regions using our secure Internet banking service.
- When sending or viewing personal or financial information online, make sure your browser's padlock or key icon is active. This icon usually appears on the bottom navigation bar of your browser window when you are using a secured site.

Important information about "phishing" and e-mail scam

Regions does not contact customers via e-mail to verify or request security information. However, some people have received fraudulent or what is now called either "spoofing" or "phishing" e-mails that have illegally used the Regions name, logo, Web site design and/or graphics. The purpose of these fraudulent e-mails is to get the recipient to divulge personal information in order to commit identity theft. In most cases, these fraudulent e-mails request the recipient to send personal information (such as Social Security or account numbers) back to the sender via e-mail; in other cases, they include a link to a Web site, which will request the visitor to enter private information.

If you have received such a fraudulent e-mail, please forward it to phishing@regions.com. If you have replied to a suspicious e-mail and provided private information about your Regions account, contact us immediately at **1-800-REGIONS (1-800-734-4667)**.

If you believe you have been a victim of identity theft, report any suspected fraud to Regions by calling 1-800-REGIONS. You also may contact the Federal Trade Commission's Identity Theft Consumer Response Center at 1-877-IDTHEFT (1-877-438-4338) or visit www.consumer.gov/idtheft/.

For more information on how Regions protects customer privacy, visit our Web site at www.regions.com and click on Privacy Pledge. The site contains helpful information for consumers, including the addresses for Equifax, Experian and TransUnion.