Security Statement

Unity Bank of Mississippi is committed to protecting your privacy and security. **We will never initiate a request for sensitive information, such as a Social Security number, account number or PIN, from you via email.** We strongly suggest that you do not share your personal ID, password, PIN or account number with anyone.

Below are some of the safeguards we have in place to protect against security breaches in the online environment:

User ID and Password - Our system is designed to limit online account access to those possessing the User ID and Password associated with your account(s).

Encryption - We have encryption technology in place (currently, 128 bit SSL) that allows for the protection of data in transit between your computer and ours. A secure website address will begin with https:// (the "s" signifies secure). The "closed lock" icon will usually indicate whether a communication session is encrypted also.

Firewalls - Our computer systems include "firewalls" that we monitor and that are designed to protect against unauthorized access to our systems.

Timeout - Our system is designed to log you off automatically after several minutes of inactivity.

Your Account Number - Generally, we only display the last four digits of your account numbers online to prevent people looking over your shoulder from seeing the full number.

Things you should do to protect yourself online:

User ID and Password - Please follow these rules to protect yourself

- Never disclose your User ID or Password to anyone else;
- Memorize your User ID or Password, don't write them down;
- Change your password frequently;
- Don't use birth dates, names, or other easily guessed letters or numbers;
- Don't be taken in: WE WILL NEVER SEND YOU AN E-MAIL ASKING FOR YOUR USER ID OR PASSWORD.

Log-off - When you are done online, log-off (look for the log-off link we provide). We suggest you do this before you shut your computer off and before you surf to any other web sites.

e-Mail - Don't use e-mail to send us sensitive information (such as social security numbers, account numbers, etc.).

"Phishing", Spoofs, Hoaxes and other Deceptive e-Mails - Be careful when responding to e-mails that look like they are from us, a regulator or an auditor. Many thieves or hackers will send you an e-mail that will ask you to click on a link that takes you to a web site (or pop-up window) where you will be asked to "confirm", "verify", "update" or otherwise provide sensitive information (such as your account number, password, PIN, or social security number). Sometimes these e-mails will falsely say that your account will be shut down if you don't act quickly. **Don't be intimidated by these threats.** These links, web sites and pop-up windows may look like ours, but will really just take you to the thief. Clicking on one of these links can expose your computer to viruses and spyware, even if you don't supply the sensitive information they want. **WE WILL NEVER SEND YOU AN EMAIL THAT ASKS YOU TO VERIFY AN ACCOUNT NUMBER, PASSWORD, PIN OR SOCIAL SECURITY NUMBER.** If you receive such a request, it is probably fraudulent. If you have any doubts about whether an email from us is authentic, don't reply to it, open any attachments or use the link in the email. To contact First State Bank please find the applicable telephone number on the Contact Us page.

Security for your own Computer - Protect your own computer by doing these things:

- Keep your operating system and browser up to date;
- Install a personal firewall;
- Install anti-virus software and keep it up to date;
- Scan your computer for spyware on a regular basis;
- Don't download programs or files from unknown sources;
- Install a pop-up blocker from a trustworthy source;
- Disconnect from the internet when you are not online.

Additional Things you should do to protect yourself:

- Don't share your account number with anyone.
- Don't give your account number to someone over the phone especially if you did not call them. Store checks, account statements and other sensitive information in a secure place.
- Don't share your ATM, debit or credit cards with anyone.

- Review your online account information frequently and your statements promptly. Let us know right away if you see something you don't recognize.
- Balance your checkbook every month. If you don't receive a statement, let us know right away.
- Obtain and review a copy of your credit report periodically. This is one way to guard against identity theft.
- Check your mailbox everyday; don't leave your mail there for thieves to steal. Consider dropping your outgoing mail in a US Postal Service mailbox.
- Use Online Payments and sign up for eStatements.
- Don't give sensitive information to unknown callers. Hang up and call the Company you want to talk to yourself, using a phone number that you located in the Phone book or your own records. **WE WILL NEVER MAKE AN UNSOLICITED TELEPHONE CALL REQUESTING SENSITIVE INFORMATION FROM YOU.**
- Shred materials containing sensitive information before you throw them away.
- Don't carry your social security card, birth certificate or passport in your wallet or purse.
- Don't print your social security number or driver's license on your checks.

If you are a victim of Identity Theft, follow these three steps:

1. Contact the fraud departments of each of the three major credit bureaus
   And report that your identity has been stolen. Ask that a "fraud alert" be
   Placed on your file and that no new credit be granted without your approval.
   EQUIFAX - 1-800-392-7816
   EXPERIAN - 1-800-682-7654
   TRANSUNION - 1-800-888-4213
2. For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions to close these accounts.
3. File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank or credit card company needs proof of the crime at a later date.