FIRST ASSET FINANCIAL INC.

POLICY and PROCEDURES for SAFEGUARDING CONFIDENTIAL CUSTOMER INFORMATION

It is important that all persons associated with First Asset Financial Inc. (First Asset or FAF) take precautions to protect sensitive customer information against unauthorized access.

The procedures include two facets: (1) protection of physical information and (2) protection of electronic information.

Physical Information

All customer confidential information should be in a secure location with access limited to authorized personnel only. It is preferable to have physical files in a lockable file cabinet. However, having such file cabinets in an office that can be locked is allowable as long as the file cabinets are within physical view of authorized personnel.

During transporting, in cars, for example, the vehicle should be locked at all times it is not occupied by an authorized person if client information is contained within the vehicle. It is recommended that such information be locked in a trunk or if in an SUV, the "modesty panel" be employed.

Care should be taken when sending checks in the mail that the check cannot be viewed through the envelope. The check should be wrapped by another sheet to prevent the check from being identified through the envelope.

Customer files should not be left unattended while unauthorized persons are present in the office.

All documents with confidential customer information on them should be torn into pieces no greater than one inch square or shredded prior to disposal.

Electronic Information

Wireless

If using a wireless connection for a laptop or desktop computer containing customer information, the wireless unit should be in the "encryption" mode or other security device or software contained within the computer.

Shut off your wireless connectivity or remove the wireless network card if you leave your computer unattended.

Disable the wireless ad hoc mode. This is a setting that allows all wireless devices to find and communicate with other wireless devices within range.

All computers should have a “firewall” of some kind, if connected to the internet.

All computers that contain confidential customer information should have some type of “virus” protection.

When using systems, such as the Southwest Securities website, BE SURE TO LOG OFF WHEN FINISHED. Leaving the connection opens more possibilities of customer information theft. This site and other confidential sites should not be left open overnight. They should be logged off when the authorized person leaves the desk for the day or an extended period of time.

You should not share your password information with others or record such information in an easily accessible location (like a “sticky note” on the computer screen!).

Change your passwords regularly. Southwest Securities Customer Information System requires at least a quarterly change in passwords.

Be conscious of anyone “snooping” if you are using a laptop in a public place or a public computer (library, for instance).

You should not store your passwords in a file on your PC or laptop—they are at risk if your computer is serviced or stolen.

If on a network, only authorized users should be allowed to use the network and the network should have a password to access the network.

The above will be monitored annually, usually during an office examination.

The home office will be checked semi-annually, once in the first quarter and once in the fourth quarter for firewalls and virus protection. Monitoring these functions will be the responsibility of David Fanshier, who will document the check via a memo placed in the correspondence file.