

# Frontier Bank

## Security Statement

(Last Amended 12/01/2004)

**PLEASE READ THIS AGREEMENT CAREFULLY AND KEEP A COPY FOR YOUR RECORDS.**

### Online Banking Security

Frontier Bank is committed to using commercially reasonable means to make your on-line banking experience safer and more secure. While we have taken the necessary steps to put in place a security infrastructure, you also play an important role in protecting your accounts.

### Safeguards

With the combination of our security and you practicing the following safeguards, your experience online should be safe and secure:

1. After the enrollment process, we will assign and mail you a "unique" Frontier NetTeller Identification Number (ID). For business accounts, the ID will be mailed to the Primary Contact for Account(s) as identified by you on your Online Banking Enrollment Form. Business accounts require the Primary Contact for Account(s) to assume the accountability of distribution to authorized signer(s) of account(s) for the Frontier NetTeller ID and PIN. Since the system will also require you to provide a PIN, your PIN will be the last four (4) digits of your social security number (TIN) for a personal and/or sole proprietor account or an Employee Identification Number (EIN) for a partnership and/or corporate account. During your first time logging in, you'll be prompted to change the "temporary" PIN. You MUST change the "temporary" PIN at this time and you will have the option to change the Frontier NetTeller ID. Once you change the "temporary" PIN to an alphanumeric PIN, only you will know it. Be sure to keep your Frontier NetTeller PIN a secret. Do not write it down, memorize it, and never disclose it to anyone. Make sure no one watches you enter it and change your Frontier NetTeller PIN if you suspect someone may know it. It is good practice to change your PIN regularly. Frontier NetTeller will require you to change your Pin every 180 days, but you will receive a 14-day advance warning before it expires.
2. In order to provide the best performance to you when using our web site, we do not send a "no-cache" command to browsers, meaning the "Back" button on your browser will work. Always sign off before visiting other Internet sites. We automatically sign you off after 10 minutes of inactivity but if you leave the computer signed on someone else could step in and press the "Back" key and view account information.
3. If others use your computer, clear your browser in order to clear the web pages that have been stored in your hard drive. How you clear your cache will depend on your type of browser. Follow your browser instructions to "clear cache".
4. Maximize the security of your browser by reviewing the security option settings on your browser, if available. Always use the highest security settings.
5. Keep your computer clean and free from viruses by using virus protection software, such as McAfee, located at <http://www.mcafee.com/>

6. We strongly recommend that you use a browser with 128-bit encryption to conduct secure transactions over the Internet. To conduct transactions through Frontier NetTeller, we require that you use a browser with 128-bit encryption.

## **Encryption**

Browsers offer varying degrees of security, particularly in regard to encryption.

Encryption helps to protect your private information so that it cannot be intercepted or read by a third party.

Encryption is a method of scrambling information for transmission between you and the bank. A key is needed to decode the information. For example, when you request information about your account to the bank your browser encrypts the information. When the bank receives the request, it is decoded and the information is sent back to you encrypted, then your browser decodes the information to read it.

There are various levels of encryption available on browsers. In order to determine when data is being encrypted, your browser will tell you. In the bottom of your browser window, there will be an icon that tells you if your banking session is encrypted. In Netscape Navigator 3.0, a "key" icon indicates you are in a secure environment, while a "broken key" indicates the environment is not secure. In Netscape Navigator 4.0 and higher and in Microsoft Internet Explorer, a "locked padlock" will indicate a secure environment and an "unlocked padlock" will indicate the environment is not secure.

**Please note:** Some browsers have an option that allows you to save your PIN for secure sites. If this option is enabled, the browser will prompt you to "save PINs" and from that point forward the PIN you selected will be stored and the browser will sign on to online banking without requiring you to enter a PIN each time. We **STRONGLY RECOMMEND** that this option be disabled because anyone who opens your browser could access your account information without needing the PIN. If you choose to enable this option, you should make every effort to explore other lock down methods for your personal computer.

If you are currently using a browser with 40-bit encryption, **PLEASE UPGRADE NOW**. By using a 128-bit browser and digital identity verification, you are protected by a much higher encryption level.

Most browsers let you check your level of encryption:

- Netscape browsers: To check your level of encryption, go to the "View menu, select "Page Info", and look under the line that begins "Security."
- Microsoft browsers: To check your level of encryption, go to the "Help" then select "About Internet Explorer."

## **Firewalls**

We employ many strategies such as firewalls and filtering routers to help ensure unauthorized users are blocked from our computers.

## **Digital Identity Verification**

We have a digital server certificate by VeriSign that your browser uses each time you sign on to verify that you are connected to the Bank and protects your transactions over the internet.

**Monitoring**

We are constantly evaluating our security architecture to ensure that it provides the highest level of privacy and safety for bank clients. We monitor site activity for anything out of the ordinary.

**Cookies**

Cookies are messages a web server (e.g., [www.frontierbank.net](http://www.frontierbank.net)) gives to a web browser (used by you). A cookie is a way for a web site to recognize whether or not you have visited the site before. The cookie cannot be read by a web site other than the one that "set" the cookie. Most cookies only last a single session. They do not read your hard drive.

If you have further questions regarding security, please contact the Internet Banking Department at 1-888-369-0303 or by e-mail at [ibsupport@frontiernational.com](mailto:ibsupport@frontiernational.com)

