First Horizon TreasuryConnect^{SM} and BusinessConnect^{SM}

Security Features

OVERVIEW

First Horizon considers the security of your financial information a top priority. We employ extensive security measures designed to provide a safe and reliable online and mobile banking experience for all of our clients.

First Horizon's data security technology combined with employees trained to spot and mitigate unusual activity help protect the security and confidentiality of your information from compromise. Security technology advancements are continuously evolving and First Horizon is at the forefront as we frequently evaluate our security environment and update as needed to help ensure that it provides privacy and safety for our clients.

We use additional layers of authentication to verify your identity when you log in. An adaptive authentication solution along with your user ID and Password checks to see if there are any unusual indicators from a variety of information and behaviors we gather to confirm who you are. If the system detects an unusual pattern with your login, you will be prompted to answer one or more of your Security Questions. You must answer these questions correctly before being allowed to continue logging in to your online or mobile banking account.

To prevent unauthorized access to your online or mobile banking accounts when you're not using your computer or mobile device, your Online or Mobile Banking session automatically signs off after 10 minutes. Best practice would be to log off or close your browser after completing your online or mobile banking session.

SECTION ONE

I. Network Security

- **Firewalls** – All First Horizon Bank systems are protected by network security that includes perimeter and internal firewalls from leading vendors. These systems are designed to confirm that only designated, authorized traffic is allowed to access First Horizon Bank Services.
- **Intrusion Prevention** – First Horizon employs systems to monitor and block traffic that attempts to breach network security.
- **Load Balancers** – The infrastructure of our online banking system provides system availability and thwarts denial of service attacks.

II. Advanced Encryption

- First Horizon Bank supports TLS 1.2 with 256 bit encryption that secures all data entered into and transferred from TreasuryConnect.

III. Site-To-User Authentication

First Horizon Bank uses technology to assist our clients in identifying authentic First Horizon Bank web sites before they provide confidential information or enter their login information.

- **Secure Site Indicators**
    - **SSL Padlock** – All clients should verify that their browser indicates that they are on a secure site (padlock or key icon) when they perform online banking functions.
    - **Extended Validation SSL** – Most of First Horizon's client-facing web sites employ Extended Validated SSL that will provide a green address bar and additional web site ownership data.
    - **Domain Name** – Clients should always review the URL for the site they are attempting to visit to verify that they are visiting a legitimate First Horizon Bank site.

IV. User Authentication

- **Unique User ID** – User ID's cannot be duplicated within the system and require 8-13 characters.
- **Strong Password Requirement** – The password must be 8 to 64 characters long, and contain at least 3 of 4 character classes (lower, upper, number and symbol).
- **2-Factor Authentication** – For clients that perform Wire and ACH transactions, First Horizon Bank uses security tokens to provide "two-factor" authentication. This is a more robust mechanism to validate that legitimate clients are accessing online banking.
- **Authentication Risk Analysis** – First Horizon Bank employs advanced security systems to perform multilayered analysis of client authentication events. This system uses multiple characteristics of the current and past authentication events to evaluate the risk of the access event and respond appropriately. As a part of this authentication each user is required to select and answer personal challenge questions as a part of initial enrollment for TreasuryConnect.
- **Session Timeout** – The Bank sets a universal timeout to help safeguard unauthorized access on unattended computers.
- **Notifications for critical account changes** – First Horizon Bank's online banking system offers clients the ability to configure notifications to keep informed about changes affecting the security of their accounts.
- **Unique User Profiles** – Users can be assigned to specific accounts and be given specific functionality (i.e. transfers, bill pay, limits, etc.).

SECTION TWO

Clients are critical to the success of account security. First Horizon works with our clients to help create the most secure TreasuryConnect experience possible. Here are some ways the client can help create a secure environment:

I. Protect Your Access Credentials

- Keep your user IDs and passwords confidential.
- Use complex passwords that could not be easily guessed. Passwords that include common events (i.e. birthdays or anniversaries), people (child's or spouse's name) or similar values are strongly discouraged because they can be easy to guess.
- Change your passwords frequently.
- Use different passwords for each online service. If a fraudster manages to obtain your password from one service, they will frequently attempt to use the same login credentials to try other sites.

II. Practice Secure Computing

- Use Antivirus and Firewall Software.
- Keep all of your software up to date with frequent and timely application of patches.

III. Logging Out Of Websites When You Are Finished

Logging out of a computer when leaving it unattended is a common and important security practice, preventing unauthorized users from tampering with it.

- Choose to have a password-protected screensaver set to activate after some period of inactivity, requiring the user to re-enter his or her login credentials to unlock the screensaver and gain access to the system.

IV. Dedicated Computers

Many businesses use a dedicated computer for online banking functions.

- Dedicating a computer to be used only for financial transactions helps eliminate security issues related to surfing the web, email or other web-based computing.

V. Dual Approval

Many businesses use dual approval for certain transactions, such as ACH and Wire.

- Two company administrators are needed to approve transactions.
- Many businesses require transaction approvals to be conducted from a separate computer than the one from which the transaction was originated.

VI. Set Limits

Businesses should work with First Horizon to establish appropriate limits for online banking transactions.

- Users that originate or approve transactions in TreasuryConnect should have limits set based on type of service.

VII. Verification Method

Verification method is a control that utilizes a separate channel outside of online banking for verification of high risk transactions.

- Telephone or text messaging will allow you to verify changes and file authentication for an added layer of security outside of a computer.