First Security Bank

Division of Glacier Bank

Cash Management Security Features

Security Key Fob Tokens REQUIRED

During their login, users will enter a random 6 digit number generated from a key fob token that is physically in their possession.

How it works: Each user will possess a key fob token. After entering their Cash Management ID and password, users will be prompted to enter the randomly generated six digit number on the face of the key fob token.

How it affects you: Users will be responsible for storing their secure key fob token in a safe place. Online access is more secure since an external hacker would not have physical access to the key fob. Hackers can key log IDs and passwords through viruses and malware, but since the token generates a new random number every sixty seconds it is difficult for hackers to predict.

Rapport, by Trusteer Inc

Add an additional layer of security to your Online Banking protection.

How it works: Rapport is a security software application that provides online transaction protection and protection from online identity theft. You can use Rapport to protect your web browser sessions with any website that contains private or personal information.

How it affects you: Rapport is entirely transparent and does not require you to change the way you work or sign into your Online Banking. It does not require any configuration or maintenance; you simply install and browse safely. Rapport further protects specific identities and sessions.

www.trusteer.com or toll free (866) 496-6139

ACH/Wire Dual Control

ACH and Wire transactions are generated and initiated through a two step process; therefore, creating an additional level of security to mitigate errors and/or internal fraud as well as external hacker risk.

How it works: One user cannot perform two actions in a row. For instance if you create or edit a batch or wire, you could not initiate/transmit it. In order to send the batch or wire, a second user would have to login to initiate/transmit it.

How it affects you: Dual Control offers a second layer of protection as it requires to all ACH batches or Wire Transfers to have at least two users involved during the whole process. Utilizing this security feature means your company will need to designate at least two users available to process ACH batches or work with Wires.

Time Restriction

Online Banking access can be restricted to certain time periods during the day and specific days of the week that are typical for your business use.

How it works: A company may assign a time period that users may login to online banking. Schedules can be customized to individual needs. For example, users who may come into the office early may be assigned a time frame of 7 am – 5 pm. Users who prefer to work later may be assigned a time frame of 8 am – 7 pm. A company may also prevent users from logging in on weekends if this is not within their typical scope of business.

How it affects you: By selecting time periods that are typically with your company's regular work schedule, users will not be affected at all. This feature provides additional security by preventing hackers and other fraudulent attempts from gaining access to online banking outside of your company's regular hours of business.

IP Restriction

Logging into online banking is only allowed from authorized Internet Addresses; therefore, providing an obstacle to external hacking attempts.

How it works: Internet Addresses for your office, home, or other common locations will be listed as *authorized* for your online banking access. When logging in, if the IP address on the computer you are using does not match an address on that list you will receive an error stating "*You are attempting to login from an unknown source*."

How it affects you: This feature is typically invisible to a user unless they are attempting to login to a computer IP address that is not within your company's list. External hacker attempts from unauthorized internet addresses will be blocked.

E-mail Alerts REQUIRED

After an ACH batch or Wire Transfer has been initiated you can receive a confirmation e-mail notification.

How it works: After any user initiates an ACH batch or transmits a wire, an e-mail notification including a summary of the batch/wire will be sent to all users with ACH or Wire functionality.

How it affects you: Receiving this alert provides your company with peace of mind that your initiation/transmission was successful as well as increases security because you are able to quickly and easily identify unauthorized batches or wires. Should your company detect any unauthorized batches or wires contact the Online Banking Department immediately.