



Multi-Factor Authentication Frequently Asked Questions

1. What does Multi-Factor Authentication do?

Multi-Factor Authentication provides additional account protection against various forms of online fraud. While your day to day banking will remain largely unchanged, the ability of a hacker to gain unauthorized access to your account will be reduced. You can use your account as you normally would from your home or office. However, in some cases you may see a difference in how your account behaves - particularly when you are attempting to log in from a computer that you did not previously register. In this case, you will be asked to provide proof that you are the owner of the account, using a variety of verification methods.

2. What are the verification methods?

Currently, we have three different verification methods: a temporary password sent to your e-mail address, a temporary password sent to your cell phone, or we will ask you a personal secret question. During the registration process, we will ask you to choose the method you prefer. If you select cell phone text messages, please be advised that your cell phone provider may charge you for the text message. Contact your cell phone provider if you are unclear of any possible charges resulting from this service. If you select email, we strongly recommend your e-mail account have a different password from your online banking account. If you would like to verify your identity by answering a personal secret question, the answer should be difficult for strangers to guess. Therefore, pick the method that is best suited for you. You may change your verification method at any time after you log in to your account. Multi-Factor Authentication will lead you through a process similar to that during the signup.

3. What happens if I fail to verify my identity?

If you fail to verify your identity after 3 consecutive times, your account will be blocked and you will not be able to access your account from any computer for 15 minutes. If you know you cannot verify your identity (i.e. you have forgotten the answer to the secret question or do not have access to your e-mail or cell phone), please call Corporate Services at (510) 723-5831 or e-mail us at Corporate.Services@fremontbank.com.

4. Should I register the computer I am using?

You should only register the computer if it is the primary or secondary computer you use, such as your laptop, home or office computer. When you are using a public computer, such as ones at the airport, in a cafe, or library, select the option "I am using this computer once" at the computer registration step. This prevents others from potentially accessing your account again using the same computer. If you are borrowing a computer or staying at a hotel, the Multi-Factor Authentication also allows you to register a computer for a certain number of days. After that period, the computer profile will be deleted from our system and you will be asked to verify your identity if you log in again from that computer.

5. What should I do if I lose my computer?

In the unfortunate case of losing your computer, such as your laptop, you should notify us immediately by calling (510) 723-5831 or e-mail Corporate.Service@fremontbank.com and we will remove the computer from our system.

6. Does it cost anything?

Multi-Factor Authentication is Free! It is a service being offered by Fremont Bank to enhance the security of your online accounts.

7. Do I have to commit to anything?

There is no commitment required. Simply use your online account as you normally would and the system will take care of the rest.

8. How does Multi-Factor Authentication protect my online account?

Multi-Factor Authentication protects your account by recognizing a computer or a group of computers that you use regularly to access your Business Online Banking account. Access is restricted to only those computers. If you, or someone else, tries to access your account from an unrecognized computer, you will be asked to verify your identity based on the verification method you choose.

9. I travel a lot and use different computers from hotels, etc to manage my money. Not all hotel rooms have internet access and sometimes I have to go to the Business Center. Will I still be able to do this?

Yes, you can access your account through the internet using any computer. You will be asked to provide proof that you are the owner of the account, using a variety of verification methods. Furthermore, you can choose whether that computer will be used to access your account: regularly, one-time, or for a period of days if you plan on using that computer several times during your stay.

10. I log onto Business Online Banking from a laptop, work PC, and at home. How do we register multiple computers?

Multi-Factor Authentication allows you to have multiple computers registered for your account(s). After you enter your username and password to log into Business Online Banking, the software verifies whether it recognizes your computer. If it doesn't, you will be asked to verify your identity based on the verification method you choose. Once verified, you have the option of choosing the regularity in which your computer will be accessing your account information and give it a name for registering/identification purposes (i.e. Joe's Laptop, Home pc, Work).

11. If I do not accept the Multi-Factor Authentication program, what will happen to my account? Can I still use my Business Online Banking?

A grace period of 45 days will be in effect for those clients who choose not to register their computers and select the "Provision Later" option. After that time, you will be required to register your computer to access Business Online Banking. If you have any questions or concerns, you can contact our Corporate Service department at (510) 723-5831.

12. Do I need to "enable cookies" on Internet Explorer for this to work?

Yes, Multi-Factor Authentication uses a "cookie" to identify your computer when you log in. If you have your cookies disabled, you will need to add <https://online.fremontbank.com> to your Trusted Sites option under the Security tab.

To do this:

1. Open Internet Explorer.
2. Choose Internet Options from the Tools menu.
3. Click the Security tab.
4. Highlight the Trusted Sites icon by clicking on it.
5. Click the Sites button.
6. Type the Address of the trusted Web site into the Address of Web site box, as seen below.
7. Click the ADD button.
8. Click the OK button.
9. Click the OK button.

13. Do other banks require this level of security for online banking?

Yes, other banks are starting to deploy similar systems. As part of our ongoing commitment to improve online security, Fremont Bank is always evaluating the latest security technology.