Multi-factor Authentication Security Enhancement
## Contents

Overview of Multi-Factor Authentication ................................................................. 4

Establishing a First Mercantile Multi-Factor User Account ........................................ 5

Authentication Questionnaire .................................................................................. 8

- Secondary Password: ...................................................................................... 8
- Password Reminder: ......................................................................................... 8
- Verification Phrase: ......................................................................................... 8
- E-mail Address: .............................................................................................. 9
- Cell Phone or Pager Number: .......................................................................... 9
- Cell Phone or Page Carrier: ........................................................................... 9
- Notify Me via e-mail Box: ................................................................................ 9
- Notify Me via Cell/Pager: .............................................................................. 9

Logging in with Multi-Factor .................................................................................. 10

Virtual Keyboard .................................................................................................. 11

- Temporary Keys: ............................................................................................. 11

Multi-Factor FAQ..................................................................................................... 12

- What is Multi-Factor authentication Security? .................................................. 12
- Why is Multi-Factor authentication necessary? ................................................. 12
- How does it work? .......................................................................................... 12
- What are the features of Multi-Factor authentication? ...................................... 12
- How many computers may I register? ............................................................. 12
- What is a "cookie"? ......................................................................................... 12
- I don't see my “Known Phrase” on the second page when logging in. What's wrong? .......................................................... 13
- Do I need to change the settings on my computer? .......................................... 13
- How do I register additional computer(s)? ...................................................... 13
- How do I login from an unregistered computer? .............................................. 13
- Why do I have a Password as well as a Security Code and can they be the same? .............................................................. 13
Help, I am attempting to login from an unregistered PC and forgot my Security Code?..................................................13

The login screen is requesting a temporary key be entered, why? .................................................................13

What happens if my Enhanced Login Security cookie is deleted or blocked by my anti-virus program? ..........14

Can I update/change my Enhanced Login Security settings once they have been established? .....................14

What happens if I enter an incorrect Password?....................................................................................................14
Overview of Multi-Factor Authentication

The Federal Financial Institutions Examination Council (FFIEC) has determined that the security provided by a single password may be defeated with new technology being employed by high-tech hackers of today. In response, regulators have mandated that enhanced security precautions be implemented to increase online safety and make accounts more secure while preventing spoofing attempts by look-a-like websites.

First Mercantile has implemented a Multi-Factor authentication security method to accounts accessed through our websites which will provide our Investment Consultants and Administrators an additional layer of protection from fraud by using more than one method to confirm user identity.
Establishing a First Mercantile Multi-Factor User Account

Upon logging into an account at the FirstMerc.com website using an existing username and password, the user will be directed to the Investment Consultants or Administrator (TPA) Multi-Factor account registration page pictured below.

Here the user will be prompted to enter his existing Investment Consultant or Administrator account password.

When a user enters his password and clicks on the “Continue” button, he/she will have the option of authenticating that computer for use with the Multi-Factor system. However, for security reasons, it is recommended that the user only authenticate computers that are private and only used by the user (e.g. his office computer) as it is easier to access an account from a computer that has been authenticated.
Upon submitting the existing password at the login, the user will be directed to the Computer Authorization page, depicted below:

This screen will allow the user to authenticate the current computer for access to his Investment Consultant or Administrator account. If a user chooses to not authenticate the computer, each subsequent time the user logs in from that computer he will have to submit his secondary password via the Virtual Keyboard. [See: Virtual Keyboard] Users not authenticating the current computer may continue to the Authentication Questionnaire section of this manual.
If the user does choose to authenticate his computer he may do so by checking the “Authenticate this computer now” box at the bottom of the screen, depicted above, and clicking on the “Continue” button. This will lead to a page where the computer will be authenticated automatically, depicted below. Once authenticated, the user will be directed to fill out the Authentication Questionnaire.
Authentication Questionnaire

The Authentication Questionnaire is automatically accessed the first time a user logs in to the Multi-Factor page and can be accessed from that point on by checking the “Change Two-factor Settings” checkbox at the login screen. It is comprised of several fields used to adjust the user’s password and notification settings as described below:

Secondary Password: This is the backup password that a user will enter when logging in from a computer that has not been authenticated. When logging in from an unauthenticated computer, the user will input this password through the Virtual Keyboard. Users are encouraged to choose a password consisting of both numbers and letters that is both distinct enough that it can be easily remembered and ambiguous enough to be secure. Users are discouraged from using simple words, names, or personal information such as addresses, social security number, or previously used passwords.

Password Reminder: This should be an inconspicuous description of the user’s secondary password. It is used to remind the user of his secondary password.

Verification Phrase: The Verification Phrase is a phrase that will be displayed whenever he logs in from an authenticated computer. This is designed to discreetly alert the user that he is logging in from an authenticated computer. If the phrase does not match what was previously entered into the system, the user should stop immediately and contact First Mercantile.
**E-mail Address:** This field is used if a user would like to receive a notification in his e-mail each time his Investment Consultant or Administrator account is accessed. This will alert the user if his account has been breached. Also, in the event that a user has forgotten his secondary password, a temporary key can be generated and sent to this e-mail address. [See: Virtual Keyboard - Temporary Keys]

**Cell Phone or Pager Number:** For an added level of security, a user may enter his cellular/pager number to have a text message sent to his cellular/pager each time the Investment Consultant or Administrator account is accessed. This would provide the user with a notification in the event of a breach of his Investment Consultant or Administrator account. Also, in the event that a user has forgotten his secondary password, a temporary key can be generated and sent to this cellular/pager. [See: Virtual Keyboard - Temporary Keys]

NOTE: Users should refer to their cellular service provider’s service plan before checking this box as some providers charge per message sent for text and page messages. First Mercantile is not responsible for charges incurred due to text messages or pages sent.

**Cell Phone or Page Carrier:** This is where a user must choose their cellular service provider or paging provider. Failure to select the proper provider will result in an inability to receive text messages and/or pages.

**Notify Me via e-mail Box:** This box can be checked to generate an e-mail to the user each time the Investment Consultant or Administrator account is accessed. This will also enable the e-mail to receive temporary keys if necessary.

**Notify Me via Cell/Pager:** This box can be checked to generate a text message or page to the provided cellular/pager number each time the Investment Consultant or Administrator account is accessed. This will also enable the user to receive temporary keys if necessary.

NOTE: Users may choose to receive notifications by e-mail, cell/pager, or both, by checking either or both “Notify Me” boxes.
Logging in with Multi-Factor

Now that the Multi-Factor account has been established, logging into the user’s FirstMerc.com online account is a simple process. The user will enter his username in the field provided by the FirstMerc.com webpage and will be directed to the following login screen depicted below:

If the computer that is being used has been authorized, the Verification Phrase entered in the Authentication Questionnaire is now highlighted in red at the top of the login screen. This means that the user needs only to enter his existing account password to access his account.

If the Verification Phrase is absent, the computer the user is currently operating has not been authenticated. Therefore, when the user submits his existing account password, he will be directed to the Virtual Keyboard for further verification. [See: Virtual Keyboard]

NOTE: Once the Multi-Factor account has been established, the user may change any information in the Authentication Questionnaire by checking the “Change two-factor settings” box on this page before logging in.

Upon submitting the password and secondary password (if necessary) the user will be logged in to his Investment Consultant or Administrator account. He is now free to utilize the Investment Consultant or Administrator account as normal.
Virtual Keyboard

Each time that a user logs in from a computer that has not been authenticated, the user will be required to enter his secondary password information via the “Virtual Keyboard” depicted below:

The “Virtual Keyboard” provides an added layer of security over conventional keyboard password entry fields by nullifying the effectiveness of keystroke logging software. The user will enter his existing secondary password here (defined in the Authentication Questionnaire) by clicking on each of the key buttons in succession to construct the password. The 16 available characters will include all necessary letters or symbols essential to complete the password. When the password has been entered correctly, press the “Continue” button to submit the password. This will direct the user through to the Investment Consultant or Administrator account.

Temporary Keys

In the event that a user has forgotten his secondary password, the user may submit a request to have a temporary key sent to his e-mail address. This request is generated by clicking on the “Click Here” link located directly to the right of the red “Forgot your secondary Password” text at the bottom of the Virtual Keyboard page, as depicted above.

If the user did not provide a valid e-mail address or cellular/pager number in the Authentication Questionnaire, then he must contact First Mercantile for assistance.
Multi-Factor FAQ

What is Multi-Factor authentication Security?
Multi-Factor authentication is a new feature for online accounts that gives you and your accounts an additional layer of protection from fraud by using more than one method to confirm your identity.

Why is Multi-Factor authentication necessary?
The Federal Financial Institutions Examination Council (FFIEC) has determined that the security provided by a single password may be defeated with new technology being employed by today’s high-tech hackers. In response, regulators have mandated that enhanced security precautions be implemented to increase online safety and make accounts more secure while preventing spoofing attempts by look-a-like websites.

How does it work?
Once the new feature becomes available, the FirstMerc.com website login will only ask for a user id. Your password will be requested on the second screen. The user id and password will be validated. Then, you will be asked to register your computer and complete a simple questionnaire, or select "Not right now, please remind me later" to login immediately. This allows users to complete the registration process at a more convenient time from a trusted computer.

What are the features of Multi-Factor authentication?
Features of this new security include:

- Registration of your primary or other trusted computer to allow express logon.
- Selection of a known phrase so as to insure that you are on a site you know. The unique phrase is only visible when logging on from a registered computer.
- The ability to logon from other computers using a Security Code or Temporary Key.
- An option to receive an e-mail upon every logon or attempt.

How many computers may I register?
You may register as many computers as you wish, but caution must be taken not to register computers accessible by others not authorized to access your accounts (e.g., shared computers).

What is a "cookie"?
A cookie is data sent to your computer by a web server that records your actions on a particular website. It is a lot like a preference file or a profile. When you visit the site after being sent the cookie, the site will load certain pages according to the information stored in the cookie.
I don't see my “Known Phrase” on the second page when logging in. What's wrong?
The Known Phrase only appears on a registered computer. It is recommended that you always login from a trusted registered computer. Caution should be taken if you do not see this phrase. If you wish to register additional computers, you will be given a chance to do so after you have entered your Security Code using the virtual onscreen keyboard and mouse or entering a requested temporary key. Note: The known phrase may not appear on a previously registered computer if you periodically delete cookies from your PC.

Do I need to change the settings on my computer?
You may need to change your Internet privacy and/or security settings to accept third-party cookies for all sites or, if possible, specifically for the FirstMerc.com website.

How do I register additional computer(s)?
When you login to the FirstMerc.com Investment Consultant or Administrator website from an unregistered computer, you will be asked if you wish to "Register this computer now" after entering your Security Code using the onscreen keyboard and your mouse. It is that easy!

Note: We do not recommend registering computers accessible by others not authorized to access your accounts.

How do I login from an unregistered computer?
When you attempt to access the FirstMerc.com Investment Consultant or Administrator website from an unregistered computer without the secure cookie, you will be asked to enter your Security Code using the onscreen keyboard and your mouse. Correctly typing in the Security Code allows you to access the FirstMerc.com Investment Consultant or Administrator website.

Why do I have a Password as well as a Security Code and can they be the same?
Your PASSWORD is used to access the FirstMerc.com Investment Consultant or Administrator website while a Security Code is used during the login process if logging in from an unregistered computer. It is not recommended that you use the same alpha-numeric string for both your PASSWORD and Security Code.

Help, I am attempting to login from an unregistered PC and forgot my Security Code?
No problem, just start the login process and refresh your memory with the Reminder that appears just above the virtual onscreen keyboard. If the Reminder does not help use the "Click here to Request Temporary Key" located under the onscreen keyboard. A temporary key will be sent to you via e-mail depending on your preference settings. Once you receive this key, log back in with your User ID, Password and Temporary Key. Note: A temporary key is valid for approximately one (1) hour and can only be used once.

The login screen is requesting a temporary key be entered, why?
A temporary key entry field is visible if one was requested within the last hour. This field will no longer be visible once you successfully login. You may either enter the temporary key received via e-mail or if you remember your Enhanced Security Code simply enter your user id and website password then click continue to reveal your
Reminder and Security Code Onscreen Keyboard to login. Note: The use of a mouse is required to select your code’s characters from the onscreen Virtual Keyboard.

**What happens if my Enhanced Login Security cookie is deleted or blocked by my anti-virus program?**

At this time, Enhanced Login Security will be disabled and you will need to register the computer(s) again or access the FirstMerc.com Investment Consultant or Administrator website by using your Security Code or the Temporary Key feature.

**Can I update/change my Enhanced Login Security settings once they have been established?**

Yes. You can update your settings by selecting "Change my settings" located on the second login screen under the Password field. Once you have been authorized, you will be given the opportunity to change and save your settings.

**What happens if I enter an incorrect Password?**

If you attempt to login with the wrong PASSWORD an error message will be displayed. Return to the login screen to try again. You can attempt to login five times before your FirstMerc.com Investment Consultant or Administrator website account is frozen.

If your account is frozen, you will need to contact a First Mercantile Client Services Representative to reconfirm your identity and have your account unfrozen.