

Dear Online Banking Client,

Premier Bank, Premier Bank Rochester and Premier Bank Minnesota are upgrading the Online Banking login process on **May 5, 2013**, in order to enhance security and protect your financial information. These new security enhancements will change how you login to Online Banking, but will continue to allow you anytime / anywhere access to your financial information and will better protect your sensitive data.

Streamlined Login Process

After the upgrade, you will notice the picture and phrase that previously appeared at login have been removed. In addition, you are no longer required to formally register your computer; the new system has technology to recognize if your computer has been used before to access the system. A more secure and behind the scene process to validate your device (PC, laptop, tablet, mobile phone), username and password will be implemented.

Enhanced Security Settings

Additional layers of security are also being added in the event you log in from a device that has not been used in the past. Instead of simple challenge questions, you will be asked to validate your identity through a one-time security code via a phone call or SMS message. These enhanced security features help safeguard your information.

Please review the additional information included in this document. If you have questions, feel free to contact a member of our Product Support team at:

(651) 777-7700, (507) 285-3700 or (800) 772-6497.

Thank you for banking with Premier Banks!

WHAT IS CHANGING?

- **PassMark is removed.** All of the security features associated with the current login process (the PassMark picture, phrase and challenge questions) will be removed, and users will no longer be asked if they want to register their computers.
- ★ **Device ID is added.** The new system has technology to recognize if the computer has been used before to access the system. It will implement a more secure and behind the scenes process to validate the device (PC, laptop, tablet, mobile phone), username and password.
- ★ **Out-of-Band Authentication is added.** Additional layers of security are being added in the event that users log in from a device that has not been used in the past. Users will be asked to validate their identity through a one-time security code via a phone call or SMS message.

One-Time Security Code

Enter the security code

We have sent a text message with a one-time security code to XXX-XXX-1234. Once you receive the message, enter the security code and click Submit.

Please note that text messages can take a few minutes to be received.

One-time security code:

[I didn't receive a text message](#)

Users will not be able to successfully complete the Out-of-Band Authentication process without at least one valid phone number recorded in Online Banking.

WHY IS IT CHANGING?

The changes are necessary to enhance the security of Online Banking and to meet the recommendations of the FFIEC Guidance *Supplement to Authentication in an Internet Banking Environment* dated June 28, 2011.

WHO IS AFFECTED?

All Online Banking users

WHEN IT IS CHANGING?

May 5, 2013

Why is it called Out-of-Band Authentication?

Out-of-Band means the authentication takes place using two channels: internet and phone.

With PassMark authentication, the internet was the only channel used.

Login Is Not Challenged:

1. Customer enters their *correct* User ID from a device (PC, laptop, tablet, mobile phone) that is typical for them.
2. Customer enters their *correct* password.
3. Customer accesses their Online Banking information.

Login Is Challenged:

1. Customer enters their correct User ID from a device (PC, laptop, tablet, mobile phone) that is not typical for them.
2. Customer is presented with a “Tell us where to reach you” dialog prompting them to select a phone number to use for Out-of-Band Authentication.
3. Customer is presented with the “Enter the security code” dialog and elects to receive a phone call or text message for Out-of-Band Authentication.
 - a. If the customer elects to receive a phone call, the customer will be asked to speak or enter the displayed one-time security code. The customer has three attempts to correctly enter or speak the security code.
 - b. If the customer selects the text message option, the “Enter your mobile phone number” dialog will be displayed. If the number entered matches a number on record, a text message containing a one-time security code is sent to the customer’s phone and the “Enter the security code” dialog is displayed.
4. After the security code is successfully entered, the customer will be able to proceed to the Password page.
5. Customer enters their *correct* password.
6. Customer accesses their Online Banking information.

One-Time Security Code

Tell us where to reach you

We need to call or send a text message to complete this process. Please tell us where you can be reached.

Phone:

- (XXX) XXX-1234
- (XXX) XXX-5678 x519872
- XX(XX)XX-XX-56-78

Text message:

- Send a text message to a mobile phone on record.

Note: Standard text message rates apply. Please contact your wireless carrier for details.

My phone number is not listed

Other Exceptions:

Lockouts will continue to occur when customers enter an invalid password beyond allowed retries. Lockouts will not occur when device IDs are rejected or customers do not successfully complete Out-of-Band Authentication.

If the customer enters an invalid User ID, a “harvesting prevention” program will take the user to the start of the Out-of-Band Authentication process where phone numbers listed are invalid and the process cannot be completed.