

Bank of Ontario branches at Genoa State Bank & Westby State Bank

Online Banking Enrollment Information

These instructions have been compiled to aid you in activating your online banking account. To complete the activation you will need your login information available.

I. Accessing the Website

To get to the Bank's website enter the link below into your browser's address bar.

<http://myvernoncountybank.com/>

From there you can click on the **Login On-Line Banking** link, also feel free to browse around the website.

Once you have received your login information follow the steps below to setup online banking.

II. Getting Started

Upon activation of your Online Banking account, a User ID and a first-time password will be provided to you. This prevents fraudulent internet authorization of the account. To start the first-time login process navigate to the Login screen, enter your User ID, and click **Submit**.

The next screen will prompt you to enter your first-time password. After entering your password and selecting whether or not your computer is public or trusted, click **Submit**.

III. Personalizing your Online Banking Login

Once you've logged in for the first time, you will be directed through a three-section process to personalize your MultiKey security authorization features.

i. Challenge Questions

Challenge questions add an extra layer of authentication to protect your Online Banking accounts. They will only appear if a login attempt is made from an unsecured or public computer. To set up your challenge questions, choose and answer three questions from the drop-down lists. Answer all of the challenge questions, answers are not case sensitive. After you have answered all three questions, click **Submit**.

ii. Challenge Image

Unlike the challenge questions, you must correctly identify the challenge image every time you attempt to login to Online Banking. This security measure is designed to protect against internet attacks that break text-based codes. The challenge images are organized into

thematic sets. Therefore, someone attempting to guess your challenge image would not only have to guess the correct image, but also the correct thematic set.

To select your challenge image, complete the following steps:

- 1) Choose the theme of your image set by clicking on one of the categories.
- 2) Select one challenge image. You will always have to select this image to login.
- 3) Click **Submit**.
- 4) A confirmation screen will appear and request that you confirm your image choice.
- 5) After confirming your selection, click **Submit**.

iii. Changing Your Login Password

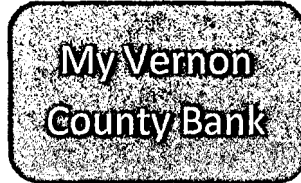
The final step of the login set up process is to create a new password. Following the challenge image confirmation, the Online Banking system will prompt you to change the password provided to you by your financial institution. Your new password must meet the requirements listed on the Create Password page. You will be asked to type your new password twice to ensure accuracy and conformity with the password requirements. After selecting the Change Password button, the password will be valid for all subsequent logins.

Bank of Ontario, Genoa State Bank & Westby State Bank

Mobile Banking App

Download Step by Step Guide

- 1.) Download the App in either the App Store (Apple) or the Play Store (Android)
Search for "Bank of Ontario" OR "Genoa State Bank" to find the App



- 2.) Once the App has been downloaded and opened, the user will be prompted to enter their Online Banking user ID, answer a challenge question, choose their image, and enter their password.
- 3.) The mobile banking user will then need to agree to the Terms of Use and Privacy agreements.
- 4.) Next go into the menu icon (three bars) in the top right corner of the screen and select settings. Here you will be able to set your log in preferences (pin, swipe, facial recognition/finger printer, or full log-in) and turn on the Snap Balance feature.

Bank of Ontario, Genoa State Bank & Westby State Bank

Mobile Check Deposit

How to Make a Successful Deposit

- 1.) Remember to sign the back of the check **FOR MOBILE DEPOSIT ONLY, DATE, ACCOUNT NUMBER, AND SIGNATURE.**
- 2.) High-quality photos of the check are the best way to make Mobile Deposit quick and easy.
- 3.) Make sure to have good lighting and a dark background.
- 4.) Only the check should be visible, no other objects or edges.
- 5.) The check needs to be entirely in the frame.
- 6.) The larger the check appears in the picture, the more likely that Mobile Deposit will verify it.
- 7.) Funds deposited from your phone may not be immediately available. Deposits made after 2 P.M. and on holidays and weekends will be posted the next business day.
- 8.) After a successful deposit, we encourage you to write on the front of the check "Mobile Deposited on MM/DD/YYYY)." We also encourage you to keep the check for 14 days. After day 14 we advise you to shred the check.

Conducting Your Transactions Online

Federal financial regulators are reporting that Internet threats have changed significantly over the past several years. Sophisticated hacking techniques and growing organized cyber-criminal groups are increasingly targeting financial institutions, compromising security controls, and engaging in online account takeovers and fraudulent electronic funds transfers.

In order to help ensure the security of your online transactions, we want you to know that:

- We will never email, call or otherwise ask you for your user name, password or other electronic banking credentials
- You can help protect yourself by implementing alternative risk control processes like:
 - Making sure you choose an adequate user name and password that, at a minimum, mixes in small case letters, upper case letters and numbers
 - Periodically changing your password (e.g., at least every 90 days)
 - Safeguarding your user name and password information
 - Making sure you have a firewall in place when conducting your financial transactions
 - Logging off the system when you're done conducting business (don't just close the page or "X" out of the system)
 - Monitoring your account activity on a regular basis

In addition, we may require owners of commercial accounts to perform their own risk assessments and controls evaluations. For example:

- Make a list of the risks related to online transactions that your business faces including
 - Passwords being written down and left out in the open
 - The use of old or inadequate passwords
 - The possibility of internal fraud or theft
 - Delays in terminating the rights of former employees
 - The lack of dual control or other checks and balances over individual access to online transaction capabilities
- An evaluation of controls your business uses may include
 - Using password protected software to house passwords in
 - Conducting employee background checks
 - Initiating a policy and process to terminate access for former employees
 - Segregating duties among two or more people so no one person has too much access or control
 - Conducting internal or third party audits of controls
 - Using firewalls to protect from outside intrusion or hackers

Federal regulations provide consumers with some protections for electronic fund transfers. These regulations generally apply to accounts with Internet access. For example, these federal laws establish limits on a consumer's liability for unauthorized electronic fund transfers. They also provide specific steps you need to take to help resolve an error with your account. Note, however, that in order to take advantage of these protections, you must act in a timely manner. Make sure you notify us immediately if you believe your access information has been stolen or compromised. Also, review your account activity and periodic statement and promptly report any errors or unauthorized transactions. See the Electronic Fund Transfer disclosures that were provided at account opening for more information on these types of protections. These disclosures are also available online (or ask us and we will gladly provide you with a copy).

If you become aware of suspicious account activity, you should immediately contact the authorities and contact us at the number listed below.

BANK OF ONTARIO
BRANCHES AT GENOA STATE BANK & WESTBY STATE BANK
(608) 337-4406 (608) 689-2655 (608) 634-6600

IMPORTANT ACCOUNT INFORMATION FOR OUR CUSTOMERS

from

**Bank of Ontario
315 Main St
Ontario, WI 54651
(608)337-4406**

ELECTRONIC FUND TRANSFERS YOUR RIGHTS AND RESPONSIBILITIES

Indicated below are types of Electronic Fund Transfers we are capable of handling, some of which may not apply to your account. Please read this disclosure carefully because it tells you your rights and obligations for the transactions listed. You should keep this notice for future reference.

Health Savings Accounts (HSA) - Health Savings Accounts (HSA). We permit you (as described below) to access your HSA with a card. This service is offered for the convenience of managing your HSA. However, electronically accessing your HSA - for example, getting additional cash back on an HSA debit card transaction - can raise a variety of tax concerns. As a result, before electronically accessing your HSA make sure you are using the correct card. Also, it is your responsibility to ensure the contributions, distributions, and other actions related to your HSA, comply with the law, including federal tax law. As always, we recommend consulting a legal or tax professional if you have any questions about managing your HSA. The terms of this disclosure are intended to work in conjunction with the HSA Agreement provided to you earlier. In the event of a conflict, the terms of the HSA Agreement control. You understand that your HSA is intended to be used for payment of qualified medical expenses. It is your responsibility to satisfy any tax liability resulting from use of your HSA for any purpose other than payment or reimbursement of qualified medical expenses. We do not monitor the purpose of any transaction to or from your HSA. Nor are we responsible for ensuring your eligibility for making contributions or ensuring withdrawals are used for payment or reimbursement of qualified medical expenses. Refer to your HSA Agreement for more information relating to the use of your HSA.

Electronic Fund Transfers Initiated By Third Parties - You may authorize a third party to initiate electronic fund transfers between your account and the third party's account. These transfers to make or receive payment may be one-time occurrences or may recur as directed by you. These transfers may use the Automated Clearing House (ACH) or other payments network. Your authorization to the third party to make these transfers can occur in a number of ways. For example, your authorization to convert a check to an electronic fund transfer or to electronically pay a returned check charge can occur when a merchant provides you with notice and you go forward with the transaction (typically, at the point of purchase, a merchant will post a sign and print the notice on a receipt). In all cases, these third party transfers will require you to provide the third party with your account number and financial institution information. This information can be found on your check as well as on a deposit or withdrawal slip. Thus, you should only provide your financial institution and account information (whether over the phone, the Internet, or via some other method) to trusted third parties whom you have authorized to initiate these electronic fund transfers. Examples of these transfers include, but are not limited to:

- **Preauthorized credits** - You may make arrangements for certain direct deposits to be accepted into your checking or savings.
- **Preauthorized payments** - You may make arrangements to pay certain recurring bills from your checking or savings.
- **Electronic check conversion** - You may authorize a merchant or other payee to make a one-time electronic payment from your checking account using information from your check to pay for purchases or pay bills.
- **Electronic returned check charge** - You may authorize a merchant or other payee to initiate an electronic funds transfer to collect a charge in the event a check is returned for insufficient funds.

Debit Card ATM transactions - types of transactions - You may access your account(s) by ATM using your Debit Card and your personal identification number (PIN) (as applicable) to:

- withdraw cash from checking or savings
- transfer funds from checking, savings to savings, checking
- get balance information about checking or savings

Some of these services may not be available at all terminals.

Debit Card point-of-sale transactions - types of transactions - You may access your checking account(s) using your Debit Card to do transactions that participating merchants will accept, including:

- purchase goods in person, by phone, or online
- pay for services in person, by phone, or online
- get cash from a participating merchant or financial institution

Currency Conversion and International Transactions - When you use your VISA(R) debit card at a merchant that settles in currency other than US dollars, the charge will be converted into the US dollar amount. The currency conversion rate used to determine the transaction amount in US dollars is either a rate selected by Visa from the range of rates available in wholesale currency markets for the applicable central processing date, which rate may vary from the rate Visa itself receives, or the government-mandated rate in effect for the applicable central processing date. The conversion rate in effect on the processing date may differ from the rate in effect on the transaction date or posting date.

Visa USA charges us a .8% International Service Assessment on all international transactions, regardless of whether there is a currency conversion. If there is a currency conversion, the International Service Assessment is 1% of the transaction. The fee we charge you for international transactions/currency conversions is disclosed separately. An international transaction is a transaction where the country of the merchant is outside the USA.

Advisory Against Illegal Use - You agree not to use your Debit Card for illegal gambling or other illegal purposes. Display of a payment card logo by, for example, an online merchant does not necessarily mean that transactions are lawful in the jurisdiction in which you may be located.

Computer access plan - types of transfers - You may access your accounts at www.myvernoncountybank.com and using your personal identification number (PIN) and User ID to:

- transfer funds from checking, savings, money market savings to checking, savings, money market savings, loans
- get balance information about checking, savings, certificate of deposit or Loans
- get withdrawal history about checking, savings or certificate of deposit
- get deposit history about checking, savings or certificate of deposit
- get transaction history about checking, savings, certificate of deposit or Loans

Limits and fees - Please refer to our fee disclosure for information about fees and limitations that may apply to these electronic fund transfers.

ATM Operator/Network Fees - When you use an ATM not owned by us, you may be charged a fee by the ATM operator or any network used (and you may be charged a fee for a balance inquiry even if you do not complete a fund transfer).

Documentation

Terminal transfers - You can get a receipt at the time you make a transfer to or from your account using an automated teller machine or point-of-sale terminal. However, you may not get a receipt if the amount of the transfer is \$15 or less.

Preauthorized credits - If you have arranged to have direct deposits made to your account at least once every 60 days from the same person or company:

- the person or company making the deposit will tell you every time they send us the money.
- you can call us at (608)337-4406 to find out whether or not the deposit has been made.

Periodic statements - You will get a monthly account statement from us for your checking account(s).

For passbook accounts, if the only possible electronic transfers to or from your account are preauthorized credits, we do not send periodic statements. You may bring your passbook to us and we will record any electronic deposits that were made since the last time you brought in your passbook.

You will get a monthly account statement from us for your savings account(s), unless there are no transfers in a particular month. In any case, you will get a statement at least quarterly.

If you do not have a checking account with us, you will get a monthly account statement from us for your savings account, unless there are no transfers in a particular month. In any case, you will get a statement at least quarterly. If you have a checking account with us, you will get a monthly account statement from us for your checking and savings accounts.

Preauthorized Payments

Right to stop payment and procedure for doing so - If you have told us in advance to make regular payments out of your account, you can stop any of these payments. Here is how:

Call or write us at the telephone number or address listed in this disclosure in time for us to receive your request three business days or more before the payment is scheduled to be made. If you call, we may also require you to put your request in writing and get it to us within 14 days after you call.

Notice of varying amounts - If these regular payments may vary in amount, the person you are going to pay will tell you, 10 days before each payment, when it will be made and how much it will be. (You may choose instead to get this notice only when the payment would differ by more than a certain amount from the previous payment, or when the amount would fall outside certain limits that you set.)

Liability for failure to stop payment of preauthorized transfer - If you order us to stop one of these payments three business days or more before the transfer is scheduled, and we do not do so, we will be liable for your losses or damages.

Financial Institution's Liability

Liability for failure to make transfers - If we do not complete a transfer to or from your account on time or in the correct amount according to our agreement with you, we will be liable for your losses or damages. However, there are some exceptions. We will not be liable, for instance:

- (1) If, through no fault of ours, you do not have enough money in your account to make the transfer.
- (2) If you have an overdraft line and the transfer would go over the credit limit.
- (3) If the automated teller machine where you are making the transfer does not have enough cash.
- (4) If the terminal or system was not working properly and you knew about the breakdown when you started the transfer.
- (5) If circumstances beyond our control (such as fire or flood) prevent the transfer, despite reasonable precautions that we have taken.
- (6) There may be other exceptions stated in our agreement with you.

Confidentiality

We will disclose information to third parties about your account or the transfers you make:

- (1) where it is necessary for completing transfers; or
- (2) in order to verify the existence and condition of your account for a third party, such as a credit bureau or merchant; or
- (3) in order to comply with government agency or court orders; or
- (4) if you give us written permission.

Unauthorized Transfers

(a) Consumer liability. (1) Generally. Tell us AT ONCE if you believe your card and/or code has been lost or stolen or if you believe that an electronic fund transfer has been made without your permission using information from your check. Telephoning is the best way of keeping your possible losses down. You could lose all the money in your account (plus your maximum overdraft line of credit). If you tell us within two business days after you learn of the loss or theft of your card and/or code, you can lose no more than \$50 if someone used your card and/or code without your permission.

If you do NOT tell us within two business days after you learn of the loss or theft of your card and/or code, and we can prove we could have stopped someone from using your card and/or code without your permission if you had told us, you could lose as much as \$500.

Also, if your statement shows transfers that you did not make, including those made by card, code or other means, tell us at once. If you do not tell us within 60 days after the statement was mailed to you, you may not get back any money you lost after the 60 days if we can prove that we could have stopped someone from taking the money if you had told us in time.

If a good reason (such as a long trip or a hospital stay) kept you from telling us, we will extend the time period.

(2) Additional Limit on Liability for VISA(R) card. Unless you have been grossly negligent or have engaged in fraud, you will not be liable for any unauthorized transactions using your lost or stolen VISA card. This additional limit on liability does not apply to ATM transactions, to ATM transactions not sent over Visa or Plus networks, or to transactions using your Personal Identification Number which are not processed by VISA.

(b) Contact in event of unauthorized transfer. If you believe your card and/or code has been lost or stolen, call or write us at the telephone number or address listed in this disclosure. You should also call the number or write to the address listed in this disclosure if you believe a transfer has been made using the information from your check without your permission.

Error Resolution Notice

In Case of Errors or Questions About Your Electronic Transfers, Call or Write us at the telephone number or address listed in this disclosure, as soon as you can, if you think your statement or receipt is wrong or if you need more information about a transfer listed on the statement or receipt. We must hear from you no later than 60 days after we sent the FIRST statement on which the problem or error appeared.

(1) Tell us your name and account number (if any).

(2) Describe the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information.

(3) Tell us the dollar amount of the suspected error.

If you tell us orally, we may require that you send us your complaint or question in writing within 10 business days.

We will determine whether an error occurred within 10 business days (5 business days for point-of-sale transactions processed by Visa and 20 business days if the transfer involved a new account) after we hear from you and will correct any error promptly. If we need more time, however, we may take up to 45 days (90 days if the transfer involved a new account, a point-of-sale transaction, or a foreign-initiated transfer) to investigate your complaint or question. If we decide to do this, we will credit your account within 10 business days (5 business days if the transfer involved a point-of-sale transaction and 20 business days if the transfer involved a new account) for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing and we do not receive it within 10 business days, we may not credit your account. Your account is considered a new account for the first 30 days after the first deposit is made, unless each of you already has an established account with us before the account is opened.

We will tell you the results within three business days after completing our investigation. If we decide that there was no error, we will send you a written explanation.

You may ask for copies of the documents that we used in our investigation.

If you have inquiries regarding your account, please contact us at:

Bank of Ontario
Pamela L. Shaw
315 Main Street
P.O. Box 9
Ontario, WI 54651
BUSINESS DAYS: Monday, Tuesday, Wednesday, Thursday and Friday
Holidays are not included.
PHONE: (608)337-4406 or (608)689-2655 or (608) 634-6600

Notice Of ATM/Night Deposit Facility User Precautions

As with all financial transactions, please exercise discretion when using an automated teller machine (ATM) or night deposit facility. For your own safety, be careful. The following suggestions may be helpful.

1. Prepare for your transactions at home (for instance, by filling out a deposit slip) to minimize your time at the ATM or night deposit facility.

2. Mark each transaction in your account record, but not while at the ATM or night deposit facility. Always save your ATM receipts. Don't leave them at the ATM or night deposit facility because they may contain important account information.
3. Compare your records with the account statements you receive.
4. Don't lend your ATM card to anyone.
5. Remember, do not leave your card at the ATM. Do not leave any documents at a night deposit facility.
6. Protect the secrecy of your Personal Identification Number (PIN). Protect your ATM card as though it were cash. Don't tell anyone your PIN. Don't give anyone information regarding your ATM card or PIN over the telephone. Never enter your PIN in any ATM that does not look genuine, has been modified, has a suspicious device attached, or is operating in a suspicious manner. Don't write your PIN where it can be discovered. For example, don't keep a note of your PIN in your wallet or purse.
7. Prevent others from seeing you enter your PIN by using your body to shield their view.
8. If you lose your ATM card or if it is stolen, promptly notify us. You should consult the other disclosures you have received about electronic fund transfers for additional information about what to do if your card is lost or stolen.
9. When you make a transaction, be aware of your surroundings. Look out for suspicious activity near the ATM or night deposit facility, particularly if it is after sunset. At night, be sure that the facility (including the parking area and walkways) is well lighted. Consider having someone accompany you when you use the facility, especially after sunset. If you observe any problem, go to another ATM or night deposit facility.
10. Don't accept assistance from anyone you don't know when using an ATM or night deposit facility.
11. If you notice anything suspicious or if any other problem arises after you have begun an ATM transaction, you may want to cancel the transaction, pocket your card and leave. You might consider using another ATM or coming back later.
12. Don't display your cash; pocket it as soon as the ATM transaction is completed and count the cash later when you are in the safety of your own car, home, or other secure surrounding.
13. At a drive-up facility, make sure all the car doors are locked and all of the windows are rolled up, except the driver's window. Keep the engine running and remain alert to your surroundings.
14. We want the ATM and night deposit facility to be safe and convenient for you. Therefore, please tell us if you know of any problem with a facility. For instance, let us know if a light is not working or there is any damage to a facility. Please report any suspicious activity or crimes to both the operator of the facility and the local law enforcement officials immediately.

MORE DETAILED INFORMATION IS AVAILABLE ON REQUEST

Bank of Ontario branches at Genoa State Bank and Westby State Bank

Online Banking Terms & Conditions

The use of Online Banking with Bank of Ontario branch at Genoa State Bank (Bank) and Westby State Bank (Bank) requires that you agree to the terms and conditions of our Service Agreement. The Agreement describes many of the features and services that Online Banking provides and how they work.

Service Charges

You will not pay any service charges or fees to view your account information or transfer funds online. If we ever change this policy, you will be notified and allowed to discontinue your service.

Receiving Online Banking Disclosures and Notices

All updates to the Service Agreement, as well as all disclosures, notices and other communications regarding Online Banking will be provided to you online. You can get free paper copies of any of these documents by calling your bank location. If you would still like to receive your paper statements they will be available.

I. General Description of Online Banking Agreement

i. What This Agreement Covers

This Agreement between you and the Bank governs the use of Online Banking services. These services permit the Bank customers to perform a number of banking functions on accounts linked to the service through the use of a personal computer.

ii. Accepting the Agreement

When you use any of the Online Banking services described by the Agreement or authorize others to use them, you agree to the terms and conditions of the entire Agreement.

iii. Relation to Other Agreements

Your use of Online Banking services may also be affected by the agreements between us for your deposit and other linked accounts. When you link an account to Online Banking services you do not change the agreements you already have with us for that account. For example, when you use Online Banking services to transfer funds between accounts, you do so under the terms and conditions we gave you in the agreement and disclosure for that account. You should review those agreements for any applicable fees, for limitations on the number of transactions you can make, and for other restrictions that might impact your use of an account with Online Banking services.

II. Online Banking Services

i. Online Banking for Consumers and Businesses

You may use Online Banking to:

- 1) Transfer funds between your linked Bank accounts, including as a payment to a linked installment loan or mortgage.
- 2) Transfer funds from your linked Bank personal or sole proprietor deposit accounts to any of your other Bank personal or sole proprietor deposit accounts.
- 3) View current balance information for your linked Bank checking, money market, savings, CD, mortgage, or loan accounts.
- 4) Review available transactions for your linked Bank checking, money market, savings accounts.
- 5) Perform self-service account maintenance, such as changing your Online ID and Online password.

**Some of the above services may not be available for some accounts.

Note: If you access Online Banking through Personal Financial Management (PFM) software or another indirect service, all of the features of Online Banking may not be available, including, but not limited to, bill presentment. To access all of the features and services offered by Online Banking, sign in directly through our Web site at www.myvernoncountybank.com.

III. Description of Online Banking Services

i. Transfers

Processing Transfer Requests

Transfers can be made between your linked Bank checking, savings, and money market accounts, or as a payment from any of those accounts to a linked installment loan or mortgage. The completion of a transfer is subject to the availability of sufficient funds at the time of final processing. If you do not have enough available funds, you may incur a non-sufficient funds (NSF) fee. Please refer to the applicable account agreement and fee schedule for details. Transfers you submit from a deposit account (checking, savings or money market) are immediately reflected in your balances for that account. Transfers entered before the cut-off time of 2:00 p.m. Central Time on a bank business day are processed on the same bank business day. Transfers entered after the cut-off time or on a non-bank business day are processed on the next bank business day.

Cut-off Times for Crediting of Transfers

The crediting of funds depends on the type of account you are transferring to and the daily cut-off time. Online Banking transfers to deposit accounts are immediately reflected in the account balance online and at ATMs. In order for transferred funds to be available to pay items that are processed against your account overnight (i.e. checks or direct debits), they must be entered before the cut-off time of 2:00 p.m. CST. To avoid possible NSF or overdraft fees, please be sure to make your transfers before the cut-off time.

ii. Online Payment Processing

Payments can be scheduled from linked checking and money market savings accounts. Payments can be entered as a one-time transaction up to a year in advance or as recurring transactions. Payments made using a checking or money market account as the funding account that are entered on our system before 2:00 p.m. on a bank business day will be scheduled and begin processing on the same bank business day. Payments made using a checking or money market account as the funding account that are entered after this cut-off time or on a day that is a non-bank business day will be scheduled and processed the next bank business day. Scheduled recurring payments that fall on a weekend or a non-bank business day will be processed on the prior bank business day. For payments to a Bank mortgage, the bank will process and credit the payment to the appropriate account effective the same business day, provided the payment is scheduled prior to the 2:00 pm CST cut-off.

iii. Limitations and Dollar Amounts for Transfers and Payments

You authorize the Bank to withdraw, debit, or charge the necessary funds from your designated Bank account on the date on which you schedule the payment to begin processing or submit a transfer request. You agree that you will instruct us to make a withdrawal only when a sufficient balance is or will be available in your accounts at the time of the withdrawal. If you do not have a sufficient balance, including available credit under any overdraft protection plan, we may refuse to complete the transaction. In either case, we reserve the right to impose NSF, over-limit or similar fees, and no further attempt will be made by the Bank to issue the payment or process the transfer request. If your payment exceeds any of the limits stated above, it will not be processed. The Bank is under no obligation to notify you if it does not complete a payment or transfer because there are non-sufficient funds or credit in your account to process the transaction. In all cases, you are responsible for making alternate payment arrangements or rescheduling the payment through the service.

iv. Canceling Payments and Transfers

You cannot cancel your transfer after it has been entered in Online Banking and the information has been transmitted to us. .

Alternative Method

However, you may request to cancel a future-dated payment scheduled through on-line service or by calling us at 608-337-4406, 608-689-2655 or 608-634-6600. You may also write to us at Bank of Ontario P.O. Box 9 Ontario, WI 54651 or Genoa State Bank P.O. Box 9 Genoa, WI 54632 or Westby State Bank P.O. Box 100 Westby, WI 54667.

We must receive your request three (3) bank business days or more before the transaction is scheduled for processing. If you call, we may also require you to put your request in writing and get it to us within 14 days after you call. If you call or write to cancel a payment that is pending, you will be charged for a stop payment in accordance with the agreement for the appropriate linked account.

v. Accounts Linked to Your Online Banking Services

When you first set up your Online ID, we will link all of your eligible accounts. If you want to limit the accounts linked or the activity level assigned to an account, please call us at 608-337-4406, 608-689-2655 or 608-634-6600 and a representative will discuss the available options with you.

IV. Monthly Service Charge

i. Monthly Service Charge

There is no monthly service charge for accessing your accounts with the Online Banking service.

ii. Other Charges

You should note that depending on how you access Online Banking, you might incur charges for:

- Normal account fees and service charges (see your account disclosures)
- Any Internet service provider fees.
- Purchase of computer programs such as Personal Financial Management (PFM) software.

NSF fees may also apply if you schedule payments or transfers and your available balance is not sufficient to process the transaction on the date scheduled.

iii. Service Hours

Online Banking services are available 365 days a year and 24 hours a day, except during system maintenance and upgrades. When this occurs, a message will be displayed online when you sign on to Online Banking.

iv. Business Days

For Online Banking services, our business days are Monday through Friday, excluding bank holidays.

v. Canceling Your Online Banking Services

If you choose to cancel your Online Banking services, any unprocessed payments will be canceled. We recommend that you cancel any scheduled payments prior to notifying us that you are discontinuing the service. The Bank will cancel any scheduled payments within two (2) bank business days from the date we receive your request to discontinue the service. If you close your primary checking account, or if it's no longer linked to your service, your Online Banking service will end, and any unprocessed payments will be canceled.

vi. Joint Accounts

When your Online Banking service is linked to one or more joint accounts, we may act on the verbal, written or electronic instructions of any authorized signer. Joint accounts using the same Online ID will be identified as one service.

vii. Changes to Agreement

We may change this agreement at any time. For example, we may add, delete or amend terms or services. We will notify you of such changes by mail or electronic message. If you maintain your Online Banking services after the effective date of a change, you indicate your agreement to the change.

viii. Cancellation

Your Online Banking services remain in effect until they are terminated by you or the Bank. You may cancel your service at any time by notifying us of your intent to cancel in writing, through Online Banking, or by calling us at 608-337-4406, 608-689-2655 or 608-634-6600. This cancellation applies to your Online Banking services, and does not terminate your Bank accounts. We recommend that you cancel any scheduled payments prior to notifying us that you are discontinuing the service. We may terminate your participation in Online Banking services for any reason, including inactivity, at any time. We will try to notify you in advance, but we are not obliged to do so.

ix. Contact by Bank

No Bank or Payee employee, nor any company affiliated with the Banks Online Banking, will contact you via email or phone requesting your Online ID or online password. If you are contacted by anyone requesting this information, please contact us immediately.

x. Reporting Unauthorized Transactions

Call us at 608-337-4406, 608-689-2655 or 608-634-6600. Online Banking customer service is available from 8:30 a.m. to 5:00 p.m., Monday through Friday, excluding bankholidays. You may also write us at Bank of Ontario P.O. Box 9 Ontario, WI 54651 or Genoa State Bank P.O. Box 9 Genoa, WI 54632 or Westby State Bank P.O. Box 100 Westby, WI 54667.

xi. Initiating Payment Inquiries

To initiate a payment inquiries please call 608-337-4406, 608-689-2655 or 608-634-6600 to speak to a customer service representative.

xii. Disclosure of Account Information

We will disclose information to third parties about your account or your transactions:

- When it's necessary for completing transfers, or to investigate or resolve a problem related to a transfer or payment.
- To verify the existence and condition of your account for a third party, such as a credit bureau or merchant.
- To comply with a government agency or court orders, or at the request of a federal regulator.
- If you give us your permission.

For more information on our Privacy Policy for Consumers, you can view it under the Privacy link at www.myvernoncountybank.com.

xiv. Account Statements

We report your Online Banking transactions on the monthly statements for your account. A description of each transaction, including the payee, the date and the amount of the transaction will appear on your statement.

V. Additional Provisions Applicable Only to Consumer and Sole Proprietors Deposit Accounts

i. In Case of Errors or Questions about Your Electronic Transactions

Call us at 608-337-4406, 608-689-2655 or 608-634-6600 or write us at Bank of Ontario P.O. Box 9 Ontario, WI 54651 or Genoa State Bank P.O. Box 9 Genoa, WI 54632 or Westby State Bank P.O. Box 100 Westby, WI 54667 AT **ONCE** if you think:

- Your statement or transaction record is wrong.
- You need more information about a transaction listed on your statement.
- An unauthorized person has discovered your Online Banking password.
- Someone has transferred or may transfer money from your account without your permission.

We must hear from you no later than 60 days after we have sent the FIRST statement on which the problem or error appeared. If you tell us verbally, we may require you to send us your complaint or question in writing or via e-mail within ten (10) bank business days. When you contact us, please provide the following information:

- Your name and account number.
- The date and dollar amount of the transaction in question.
- The name of the Payee if the transaction in question is a payment.
- The transaction number assigned by Online Banking, if available.
- A description of the transaction about which you are unsure.

Please explain as clearly as you can why you believe there is an error or why you need more information.

We will determine whether an error occurred within 10 bank business days after we hear from you, and we will promptly correct any error we have made. If we need more time, however, we may take up to 45 days to investigate your complaint or question. For errors involving new accounts, point-of-sale, or foreign-initiated transactions, we may take up to 90 days to investigate your complaint or question. For new accounts, we may take up to 20 business days to credit your account for the amount you think is in error. If we decide to do this, we will provisionally credit your account within 10 bank business days for the amount you think is in error, so that you have the use of the money during the time it takes us to complete our investigation. If we ask you to put your complaint or question in writing, and we do not receive your letter in 10 bank business days, we reserve the right not to provisionally credit your account. If we conclude there was no error, we will send you a written explanation within three (3) bank business days after we complete our investigation. You may request copies of the documents that we used in our investigation.

ii. Limitation of Liability

Tell us at once if you believe your Online Banking password has been compromised or if someone has transferred or may transfer money from your account without your permission. The best way to minimize your loss is to call us immediately. The unauthorized use of your Online Banking services could cause you to lose all of your money in your accounts, plus any amount available under your overdraft protection. You will have no liability for unauthorized transactions if you notify us within 60 days after the statement showing the transaction has been provided to you. If you do not, you may not get back any of the money you

lost from any unauthorized transaction that occurs after the close of the 60-day period, if we can show that we could have stopped the transaction if you had notified us in time. If a good reason (such as a long trip or hospital stay) kept you from telling us, we may extend the time periods. When you give someone your Online Banking ID and password, you are authorizing that person to use your service, and you are responsible for all transactions that person performs while using your service. All transactions that person performs even those transactions you did not intend or want performed are authorized transactions. If you notify us that the person is no longer authorized, then only transactions that person performs after the time you notify us are considered unauthorized.

Transactions that you or someone acting with you initiates with fraudulent intent are also authorized transactions. For your protection, sign off after every Online Banking session and close your browser to ensure confidentiality.

iii. Our Liability for Failure to Complete Transactions

If we do not complete a transaction to or from your account on time or in the correct amount according to our Agreement with you, we will be liable for your losses or damages. However, there are some exceptions. For instance, we will not be liable:

- If, through no fault of ours, you don't have enough available funds in your account (or available credit under your overdraft protection plan), or credit to cover the transaction or transfer.
- If Online Banking services weren't working properly, and you knew about the malfunction when you started the transaction or transfer.
- If circumstances beyond our control (such as fire or flood) prevented the transaction or transfer, despite reasonable precautions we've taken.
- If there are postal delays or processing delays by the Payee.
- There may be other exceptions not specifically mentioned.

VI. Additional Provisions Applicable Only to Business Accounts (Other than Sole Proprietors)

i. Protecting Your Password

You agree that we may send notices and other communications, including password confirmations, to the current address shown in our records, whether or not that address includes a designation for delivery to the attention of any particular individual. You further agree that the Bank will not be responsible or liable to you in any way if information is intercepted by an unauthorized person, either in transit or at your place of business. You agree to: 1) keep your password secure and strictly confidential, providing it only to authorized signers on your account(s); 2) instruct each person to whom you give your password that he or she is not to disclose it to any unauthorized person; and 3) immediately notify us and select a new password if you believe your password may have become known to an unauthorized person. The Bank will have no liability to you for any unauthorized payment or transfer made using your password that occurs before you have notified us of possible unauthorized use and we have had a reasonable opportunity to act on that notice. We may suspend or cancel your password even without receiving such notice from you, if we suspect your password is being used in an unauthorized or fraudulent manner.

ii. Acknowledgement of Commercially Reasonable Security Procedures

By using Online Banking, you acknowledge and agree that this Agreement sets forth security procedures for electronic banking transactions that are commercially reasonable. You agree to be bound by instructions, whether authorized or unauthorized, which we implement in compliance with these procedures, unless you have given us prior notice of possible unauthorized use as described above (and we had a reasonable opportunity to act on such notice).

iii. Limitation of Bank's Liability

If we fail or delay in making a payment or transfer pursuant to your instructions, or if we make a payment or transfer in an erroneous amount that is less than the amount per your instructions, unless otherwise required by law, our liability shall be limited to interest on the amount that we failed to timely pay or transfer, calculated from the date on which the payment or transfer was to be made until the date it was actually made or you canceled the instructions. We may pay such interest either to you or the intended recipient of the payment or transfer, but in no event will we be liable to both parties, and our payment to either party will fully discharge any obligation to the other. If we make a payment or transfer in an erroneous amount that exceeds the amount per your instructions, or if we permit an unauthorized payment or transfer after we have had a reasonable time to act on a notice from you of possible unauthorized use as described above, unless otherwise required by law, our liability will be limited to a refund of the amount erroneously paid or transferred, plus interest thereon from the date of the payment or transfer to the date of the refund, but in no event to exceed 60 days' interest. If we become liable to you for interest compensation under this Agreement or applicable law, such interest shall be calculated based on the average federal funds rate at the Federal Reserve Bank in the district where the Bank is headquartered for each day interest is due, computed on the basis of a 360-day year. Unless otherwise required by law, in no event will the Bank be liable to you for special, indirect or consequential damages including, without limitation, lost profits or attorney's fees, even if we are advised in advance of the possibility of such damages.

VII. Electronic Disclosure and Consent

You agree that we may provide you with all disclosures, notices and other communications about Online Banking, Business Online Banking, including the Online Banking Agreement and any future amendments, in electronic form. We will provide all future notices by posting them on the Online Banking Sign-In Page for a period of at least 30 days. You may download or print the notices from your computer if you have the hardware and software described below. At your request, we will provide you with a paper copy of any of the above documents without any fee. You have the right to withdraw this consent, but if you do, we will immediately terminate your participation in Online Banking and/or Business Online Banking. You may obtain copies of any documents we provided electronically or withdraw your consent by calling us at 608-337-4406, 608-689-2655 or 608-634-6600.

VIII. Your System Requirements

In order for you to access and retain records in connection with Online Banking at the Bank your system must meet the following requirements:

- Sufficient electronic storage capacity on your computer's hard drive or other data storage unit such as a table, smart phone, etc...
- An e-mail account with an Internet service provider and e-mail software in order to participate in our electronic Communications programs;
- A personal computer (for PC's; Pentium 120 Hhz or higher; for Macintosh, Power Mac 9500, Power PC 604 processor 120-MHz Base or higher), operating system and telecommunications connections to the Internet capable of receiving, accessing, displaying, and either printing or storing Communications received from us in electronic form via a plain text-formatted e-mail or by access to our web site using one of the browsers specified below:

➤ **Adobe Reader version 8.0 or higher**

➤ **If you are using a Windows operating environment**

- 1.3GHz or faster processor, Microsoft Windows **XP** with Service Pack 3 for 32 bit or Service Pack 2 for 64 bit; Windows Server 2003 R2 (32 bit and 64 bit); Windows Server 2008 or 2008 R2 (32 bit and 64 bit); Windows 7 (32 bit and 64 bit); Windows 8 or 8.1 (32 bit and 64 bit), 256MB of RAM (512MB recommended) 320MB of available hard-disk space, 1024x768 screen resolution; Firefox Extended Support Release; Chrome

➤ **If you are using a Mac OS**

- Intel processor, Mac OS X v10.6.4, v10.7.2, or v10.8, 1GB of RAM, 350 MB of available hard-disk space, 1024x768 screen resolution Safari 5.1 for Mac OS X v10.6.8 or v10.7.2; Safari 5.2 for MAC OS X v10.8; Safari 6.0 for Mac OS X v10.7.4 or v10.8

To print or download disclosures, you must have a printer connected to your PC or sufficient hard-drive space to save the disclosure.