FERGUS FEDERAL CREDIT UNION – ONLINE TERMS & CONDITIONS

ONLINE BANKING DISCLOSURE:

Fergus Federal Credit Union is confident of our system's ability to protect all transactions; however, this system is for the use of authorized users only. This is a private computing system; its use is restricted to authorized individuals only. Actual or attempted unauthorized use of this computer system will result in criminal and/or civil prosecution. We reserve the right to view, monitor and record activity on the system without notice or permission. Any information obtained by monitoring, reviewing or recording is subject to review by law enforcement organizations in connection with the investigation or prosecution of possible criminal activity on the system. If you are not an authorized user of this system or do not consent to continued monitoring, exit the system at this time.

SECURITY:

The Internet is a rapidly changing marketplace with a wide variety of products and services available online. Although consumers and financial institutions agree that there is great value in offering online services, consumers may be concerned about security.

Our online service is built on a foundation of stringent security policies, rigorously tested technologies, and a highly trained and experienced staff. Our combination of Internet expertise and in-depth knowledge and experience in the financial services industry provide a secure solution to consumer concerns. You may rest easy knowing that your financial information will be protected with state-of-the-art security every step of the way.

HOW DO I PROTECT MYSELF? :

We want your online banking experience to be enjoyable and safe. That's why we use a secure SSL encryption, constantly updated and monitored systems along with multiple security layers, firewalls, and procedures. We also want to make you aware of several straightforward security tips to keep in mind:

- ***Use a strong password***. Choose passwords that are difficult for others to guess and use a different password for each of your online accounts.
- ***Change your Passwords frequently***.
- Every time you access Online Banking your personal image and name will appear before you enter your password. Seeing your image and name will let you know that you are at our *real* site and not a fake or fraudulent site. This means it is safe to enter your password. If the correct image and name do not appear, do not enter your password and contact us immediately at 406-535-7478.
- You may be asked to set-up several security questions that only you should know the answers to. Our security system will recognize the computers you normally use to access your online banking site. In the future, if you or someone else attempts to log in to your account from a new or unrecognized computer, you may need to answer some of your security questions before being allowed to continue.
- ***Leave suspicious sites.*** If you suspect that a website is not what it purports to be, leave the site immediately. Do not follow any of the instructions it presents. For Microsoft Internet Explorer (IE) users setting your browser security setting to "high", a level that makes it more difficult to interact with some Web sites, is also recommended.

- ***Be alert for scam emails***. These may appear to come from a trusted business or friend, but actually are designed to trick you into downloading a virus or linking to a fraudulent website and disclosing sensitive information.
- Though we will communicate with you over email from time to time, we will never request that you provide sensitive or personal information via email. Don't reply to any email that requests your personal information. ***Be very suspicious of any email from a business or person that asks for your password, Social Security number, or other highly sensitive information and/or one that sends you personal information and asks you to update or confirm it.***
- Open emails only when you know the sender. Be especially careful about opening an email with an attachment. We advise that you shouldn't open attachments unless you are confident that you can trust the source
- ***Do not click on links in emails from unknown senders or on links in emails that are asking you to change or update personal information***.
- Do not send sensitive personal or financial information unless it is encrypted on a secure website. Regular emails are not encrypted and are more like sending a post card. Look for the padlock symbol to ensure that the site is running in secure mode before you enter confidential personal information.
- Don't take anything for granted and only do business with companies you know and trust. Always keep in mind that forging emails and creating phony "look alike" websites designed to trick consumers and collect their personal information is not difficult. Make sure that websites on which you transact business post privacy and security statements, and review them carefully.
- Make sure your home computer has the most current anti-virus software. Anti-virus software needs frequent updates to guard against new viruses. We recommend that you use a program that automatically upgrades your virus protection on a regular basis. If you currently do not have this automatic upgrade feature, make sure you update your virus detection program weekly and when you hear of a new virus. If your anti-virus product doesn't include spyware protection, we recommend that you install a reputable spyware detection product as well.
- When your computer is not in use, shut it down or disconnect it from the Internet.
- ***Act quickly if you suspect fraud. If you believe someone is trying to commit fraud and/ or if you think you may have provided personal or account information in response to a fraudulent email or Web site, report the incident immediately, change your passwords and monitor your account activity frequently.***

BROWSER SUPPORT:

For this online service we recommend that you use one of the following browsers:

Windows

- Chrome 29 and above
- Firefox 23 and above
- Internet Explorer 10 and above

Macintosh

- Safari 5 and above

Some areas of our site may require the use of Flash Players or Adobe Acrobat Reader. Other browsers and operating systems may work effectively, however we do not test against them; therefore your experience may vary. We regularly monitor and test browsers to ensure the highest security standards. Our site supports TLS 1.2 and up.

POP-UP WINDOWS:

It is strongly recommended that you enable the use of pop-ups for our Website. Pop-up functionality is used by many Websites to display advertisements to users, but some services like this one, use pop-up functionality to draw attention to important information.

COOKIES:

In order to provide optimal security, performance and reliability, this service requires that cookies be enabled on your Web browser. Cookies are a small piece of information that a Web server can store on your browser so the system recognizes your actions during a session.

As you browse the Web, some cookies are "set" on your Web browser. For example, cookies are used to store preferences you have requested on frequently visited Web sites. When you close your browser, some cookies are stored in your computer's memory in a cookie file, while some expire immediately. All cookies have expiration dates.

Cookies cannot be used to obtain data from your computer, get your e-mail address or access sensitive or personal information. The only way that any private information could be part of your cookie file would be if you personally provided that information to a Web site. Also, each cookie can only be read at the site where the cookie was created.

ACCOUNTS SUMMARY PAGE:

The Accounts Summary page provides a summary of your accounts and the transactions scheduled to occur within the next 30 days. You also have convenient access to important information such as the Message Center and Payment Guarantee.

MESSAGE CENTER:

In the Message Center you will have immediate access to important service updates and account alerts. You can also use the Message Center to send direct, secure messages to our Member Service team. Unlike regular Internet e-mail, these messages are protected by encryption and verification technology, so any confidential information cannot be intercepted by unauthorized persons.

READING MESSAGES:

After you log into the service, look at the Messages box in the upper right portion of the screen. You will see an envelope icon, along with a link indicating the total number of new messages and alerts you have received. If you have new messages, you can read them by clicking on the "Messages" link.

After reading a message, you can reply to it by clicking on the "Reply" button, or delete the message by clicking on the "Delete" button.

After reading an alert, you can delete it by clicking on the "Delete" button.

All messages will be kept in the Message Center for 90 days and alerts for 30 days unless you delete them.

COMPOSING MESSAGES:

From the Message Center screen, click on "Compose Message" link.

Tell us what your message is regarding by selecting the subject from the dropdown menu, then enter the content of your message in the Message box. Be sure to include as much information

as possible for inquiries about completed payment transactions. Finally, click on the "Submit" button.

DELETING MESSAGES:

Messages can be deleted by checking the check box next to the message(s) that you would like to delete and then clicking the "Delete Selected" button.

LAST LOGIN DATE / TIME:

The Last Login stamp appears on the Overview page and is a security feature designed to help monitor the access of your online accounts. Please note that the Last Login stamp will also reflect log in activity if:

- You share your User ID and Password with another person.
- You use a third-party account aggregation service that automatically logs in to your account for balance and transaction updates.

If you have questions related to the time or date your account was accessed last, please contact Member Services.

MEMBER SERVICE:

For your convenience, Member Services is available by calling 406-535-7478. You can also use the Message Center to send direct, secure messages to our Member Service team. Unlike regular Internet e-mail, these messages are protected by encryption and verification technology, so any confidential information cannot be intercepted by unauthorized persons.

Our mailing address is:

Fergus Federal Credit Union
Attention: Online Banking Member Service
106 E Janeaux
Lewistown, MT 59457

ACCOUNT ACTIVITY:

The Account Activity screen allows you to review your account statement and get information about each of your online accounts, such as checks cleared, ATM activity, deposits, and online transactions.

You can select the account to view by selecting the account in the Account drop down menu.

The default display will show you the past 30 days of transaction history. To view transactions from a different period of time, click on the "Viewing Last 30 Days" link. A window will appear where you can select a different time period to view. Some transactions may appear on subsequent pages. Use the page controls to move between pages or to display additional transactions on each page.

To change the sort order of the displayed transactions, simply click on the column you wish to sort by, such as Date, Description, Check Number (if applicable) or Amount. Click the column heading a second time to reverse the sort order.

To view additional details about the account, select the Account Details link. You can also change the account nickname as it is displayed in Online Banking here.

EXPORTING DATA:

If you like to manage your money through this service as well as another financial management software tool, you can easily export information from our service and load it into Quicken® or MoneyDesktop®. The transactions you initiate through our service can be exported into a .qif or a CSV file. Older versions of Quicken software (Quicken 2004 and earlier) and Microsoft Money can import a .qif formatted file. CSV (Comma Separated Value) files can be opened by Microsoft Excel® and other financial and spreadsheet applications.

From the Payment Activity page or Account Activity page, click on the "Export Data" link. Select the file format and date range of transactions desired. You can then save the file and import it into the software of your choice.

To view additional options available for the account selected in the drop down list, click on the “More” link.

To view the image of a check that has been paid, click on the check number in the Check column. To search for a specific check image, click on the View Check link.

ENDING YOUR ONLINE SESSION:

Click on the "Log Out" button (top right corner) to end your session. We recommend that you always click on the "Log Out" button, rather than just closing your browser window, to ensure that you are fully logged out of your secure session.

SESSION TIME-OUT:

If your online session is inactive for approximately 14 minutes (that is, if you have not submitted any transactions or clicked on any new pages), you will receive a message, warning that you will be logged off soon if there is no further activity. Clicking "Continue" upon receiving the message will allow you to proceed with your online activity and will refresh the system. If no further activity occurs, the system will automatically save and send any transactions you made and terminate the session. The online service is designed this way to provide you with maximum security in case you forget to log out.

EXPEDITED PAYMENT GAURENTEE:

If a Properly Scheduled Expedited Payment (defined below) is not received and posted by the payee as of the scheduled payment date, you will not be responsible for any Penalties (defined below) that arise due to the failure of such payment to post on the scheduled date and we will refund you the service fee associated with such payment We will first attempt to have any such Penalties removed, and if the payee is unwilling or unable to remove them, we will pay the fees and finance charges directly to the payee. In addition, we will attempt to have your payee account noted appropriately to ensure that the situation does not negatively impact your credit rating.

"Penalties" are defined as late fees or finance charges that are assessed on the Properly Scheduled Expedited Payment amount that did not post on the scheduled payment date, not those based on your total outstanding balance.

A "Properly Scheduled Expedited Payment" is defined as a payment that:

1. Was made from an account that has sufficient funds for the payment and any fees associated with the payment;
2. Was scheduled to be delivered on or before the due date of your bill, excluding any grace periods. (The one exception to this guideline is that mortgage payments may be scheduled so that the payment is sent on or before the due date including grace periods. For example, a mortgage payment due on July 1st, with a 15-day grace period, must have a "Deliver By" date no later than July 15th.);
3. The service indicates is deliverable on or prior to the applicable due date;
4. Was not made for any of the following types of transactions:

- Payments to settle securities transactions
- Payments that failed due to insufficient funds or other reasons
- Payments to payoff special or delayed financing for purchases
- Payments to credit counseling agencies who pay creditors on your behalf
- Payments to payees outside of the United States
- Court-ordered payments such as alimony, child support, speeding tickets, etc.
- Tax entities
- Collection agencies
- the information supplied by you is correct (payee name and address, your name and account number as it appears on the payee's records);
- was scheduled when the system was available; and
- The payment complies with the payee's policies.