Fraud Policy Guidelines

In the event that someone has gained unauthorized access to your credit union account through On-Line banking, our commitment is that we will reimburse you for the money that you have lost from your account provided you have met your responsibilities.

You are a vital part of the security effort. We can't do it alone. We need you to do your part in order to help us protect your information and finances. Understanding the safeguards will help you in protecting your security on-line. While we take strong measures to protect the security and privacy of your information, there are important steps that you should take to help protect your information when using the internet.

Meeting these responsibilities under your agreement with us includes the following:

1) Protecting your Personal Access Code (PAC):
- Select a PAC that is easy for you to remember but difficult for others to guess.
- Do not select a part of your PIN or other password as your PAC.
- Keep your PAC confidential and do not share it with anyone.
- Do not write down your PAC or store it in a file in your computer.
- Never disclose your PAC in a voice mail or e-mail.
- Ensure that no one observes you typing your PAC.
- Change your PAC frequently (every 90 to 120 days).

2) Protecting your Computer:
- Install an anti-spyware program. Ensure your anti-spyware is enabled and configured to run daily updates and regular spam scans.
- Install an anti-virus program. Ensure your anti-virus software is enabled and configured to run daily updates and regular virus scans.
- Install and use a personal firewall on your computer to ensure others cannot access your computer through the internet.
- Install new security patches as soon as your operating system and internet browser manufacturers make them available.
- Disable automatic password-save features in the browser and software you use to access the Internet.
- Do not use Memorize Account feature on public available computers.
- Always exit our Internet banking site using the "log out" button and close your browser if you step away from your computer. Your browser may retain information you entered in the login screen and else where until you exit the browser.
- Secure or erase files stored on your computer by your browser so others cannot read them.

3) Practice Safety pre cautions for online Banking:

- The easiest way to tell if an email is fraudulent is to bear in mind that we will never ask you for your personal passwords, personal information numbers or login information in an email.
- When banking online, check the address of any pages that ask you to enter personal account information. In the toolbar at the top of the page, any legitimate internet banking web site will begin with ‘https’ or ‘shttp’ to indicate that the page is secure.
- Look to the padlock on your screen. If the page is legitimate, by clicking on the padlock, you can view the security certificate details for the site. A fraudulent site will not have these details.
- Type in our web address yourself to ensure you are transacting with our server.
- Check your account and credit card statements regularly and carefully to ensure that all transactions are legitimate.

4) The practice of accessing your account information through publicly accessible computers and public wireless networks is strongly discouraged. The use of computers at locations such as Internet cafes, public libraries, hotel lobbies and public wireless networks such as “hotspots” to name a few examples, greatly increases the risk of possible unauthorized access to your accounts. Use of these access points are to be avoided and if it is determined to be the compromise point, this would have a negative impact on your ability to be compensated for your losses.

5) Notify the credit union immediately upon discovering or suspecting that unauthorized activity has occurred or that your PAC or PIN may have been compromised.

6) Reviewing your statements and reporting errors within the time periods set out in your agreement.

7) Fully cooperating and assisting the credit union and the law enforcement investigation in the event that you have been victimized by an online fraudulent activity or improper access to your accounts.

8) In the case of accessing Business Accounts and Services, by the act of designating a person as a Business User, the business is authorizing that person to view information about the Business and if online transactions are permitted through the service, also authorizing to carry out online transactions on behalf of the Business, the Business accepts the responsibility for all losses that may arise from a Business Users misusing his or her authority in any way, either purportedly on the Business’ behalf or for personal or other purposes. The Business and individual Business User will ensure that the Business User meets any eligibility or other requirements for online access that are communicated by us as part of the application process. The Business is also responsible for ensuring that any changes with respect to who is the authorized or designated Business User are appropriately managed by the Business and that passwords and other applicable user id or access information is managed accordingly.