# Security Statement

Security is a priority at Members First Credit Union. We maintain physical, electronic, and procedural safeguards that comply with federal guidelines to guard your personal information against unauthorized use. In addition to rigorous authentication procedures, this area of our website will provide you with information to help manage and keep your account information protected.

Your information is encrypted during the transfer between your browser and our site. This technology, called Secure Socket Layers (SSL), protects information you submit or receive through our online access site. Your browser must support SSL encryption to use our site. Newer versions of all the popular browsers are capable. Encrypted sites are designated by beginning with https: instead of just http:.

## How Members First Credit Union Protects You

Members First will continue to do our utmost best to enhance and maintain our standards of security and procedures to protect against fraudulent activity and/or access to your nonpublic information and records. These security standards will also protect former members who applied for an account or utilized our services in the past for as long as the information is retained.

For members that utilize our Online Banking, Mobile applications, or our Online Bill Pay service, you can be confident that our high levels of security will protect your personal and financial information and that you are covered in the unlikely occurrence of an unauthorized transaction. In the unfortunate event there is an unauthorized transaction on your account please contact our offices as soon as possible to ensure prompt action on your behalf.

**Firewalls**

Members First Credit Union uses firewalls to help limit entry from anyone that does not have the proper authorization. A firewall is a technological barrier designed to prevent unauthorized or unwanted communications between computer networks or hosts. It acts as a shield against data going in or out of a network and checks to ensure that communications only occur between approved individuals and that all communications are in proper protocol.

## How to Protect Yourself

While Members First continually strives to remain on top of Internet technology, Internet security is a cooperative effort, and we need your assistance. Understanding the many different types of fraud will help you avoid becoming a victim.

**Phishing**

Phishing is a type of online fraud where you are tricked into providing your personal information through your computer. It involves fraudsters who send messages to lure your personal information (credit card numbers, bank account information, Social Security number, passwords, or any other type of sensitive information) from unsuspecting victims. They do this by posing as a financial institution or another company you have an established relationship with. These types of attacks can also be referred to as SMishing or SMS Phishing, or Vishing (voice Phishing).

***At no time will Members First Credit Union ever call or email you asking for your personal information or log in credentials. If you receive a suspicious phone call or email asking you to provide your personal information, account numbers, or log in credentials you should decline to do so and contact us at 1-866-238-0277 or 608-271-5301.***

**Malware**

Malware is short for “malicious software,” this includes spyware and viruses installed on your computer, phone, or mobile device without your consent. Malware can be used to steal your personal information and account numbers, send spam emails, and commit fraud.

**Identity Theft**

Identity Theft occurs when someone uses your personal identification information, such as your name, Social Security number, address, or credit card numbers, without your permission, to commit fraud or other crimes. The Federal Trade Commission offers online assistance with steps consumers can take to protect themselves against identity theft.

To learn more about Identity Theft and what you can do to protect yourself visit the Federal Trade Commission website at www.ftc.gov

## Tips for creating strong secure passwords

Passwords provide the first line of defense against unauthorized access to your computer and personal information. The stronger the password, the more protected your information will be from hackers and malicious software. Passwords should:

- Be at least 8 characters long

- Not contain your username, real name, or company name
- Not contain a complete word
- Be significantly different from previous passwords
- Avoid using sequences or repeated characters
- Contain a mixture of characters – uppercase and lower case letters, numbers and special characters (@&$^%*)

Passwords should never be written down or saved to your computer. When your computer asks to remember your password it is recommended to click “NO.”

The best way to protect yourself from any type of fraud is to check your accounts frequently, change passwords often and report unauthorized activity immediately!