# Member Awareness Program

In a constantly changing technology environment, Merced School Employees Federal Credit Union strives to provide exceptional service to our members while safeguarding our members' assets and information. We use multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.

MSEFCU will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential member information

**Online Banking Security**

MSEFCU is committed to protecting your personal information. Our Online Banking system uses several different measures to ensure your information is protected. All information within our online banking uses the Secure Socket Layer (SSL) protocol to ensure that your account information transmitted is protected. All information transferred through Online Banking has a 256-bit encryption to make your information unreadable as it passes over the internet. Other online security measures include: automatic time out that occurs if there is no activity within the required time period, recognizing the user's computer and usage patterns, limited log-in attempts, challenge questions and security phrases.

As fraud cases are on the rise, it is also important that you take your own measures to ensure your information remains protected.

**Here are some tips on how to stay safe when conducting business online.**

- Never give out any personal information including User Names, Passwords, Social Security number, or Date of Birth
- Don't respond to email, text, and phone messages that ask for personal information. Legitimate companies don't ask for information this way.
- Create passwords that mix letters, numbers, and special characters. Don't use the same password for more than one account.
- Don't use personal information for your user names or passwords, such as birth dates or Social Security number.
- If you shop or bank online, use websites that protect your financial information with encryption. An encrypted site has "https" at the beginning of the web address; "s" is for secure.
- If you use a public wireless network, don't send information to any website that isn't fully encrypted.
- Use anti-virus and anti-spyware software, and a firewall on your computer.
- Set your computer's operating system, web browser, and security system to update automatically.

For more information: Federal Trade Commission – www.ftc.gov/idtheft

**Identity Theft**
**What is Identity Theft?**

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can wreak havoc with your finances, credit history, and reputation – and it can take time, money, and patience to resolve.

**How to protect your information**

- Never give out any personal information including birthdate, Social Security number or passwords
- Report lost or stolen checks or credit cards immediately.
- Review your credit reports. You have a right to a free credit report every 12 months from each of the three nationwide credit reporting companies. To order your report, visit annualcreditreport.com or call 1-877-322-8228.
- Read your bank, credit card, and account statements. If a statement has errors or doesn't come on time, contact the business.
- Shred all documents containing personal information: bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings and invoices.
- Don't respond to email, text, and phone messages that ask for personal info. Legitimate companies do not ask for information this way.

For more information about identity theft and other tips on how to protect your information visit:
Federal Trade Commission: http://www.ftc.gov/idtheft
Federal Deposit Insurance Corporation Consumer Alerts: www.fdic.gov/consumers/consumer/alerts
United States Department of Justice: www.usdoj.gov/criminal/fraud

**Credit Reporting Agencies**

**Equifax**
PO Box 105069
Atlanta, GA 30349-5069
www.equifax.com
To order a report: **800-685-1111**
To report fraud: **800-525-6285**

**Experian**
PO Box 2002
Allen, TX 75013-0949
www.experian.com
To order a report: **888-397-3742**
To report fraud: **888-397-3742**

**Trans Union**
PO Box 1000
Chester, PA 19022
www.transunion.com
To order a report: **800-916-8800**
To report fraud: **800-680-7289**

**Debit Card Fraud**

Debit Card Fraud takes place every day in a variety of ways. You can't always prevent it from happening, but you can create some obstacles and make it tougher for someone to get hold of your cards and card numbers. Incorporating a few practices into your daily routine can help keep your cards and account numbers safe. For example, keep a record of your account numbers, their expiration dates and the phone number to report fraud for each company in a secure place.

**Other fraud protection practices include:**

- Don't give your account number to anyone on the phone unless you've made the call to a company you know to be reputable. If you've never done business with them before, do an online search first for reviews or complaints.
- Carry your cards separately from your wallet. It can minimize your losses if someone steals your wallet or purse. And carry only the card you need for that outing.
- During a transaction, keep your eye on your card. Make sure you get it back before you walk away.
- Never sign a blank receipt. Draw a line through any blank spaces above the total.
- Save your receipts to compare with your statement.
- Open your bills promptly — or check them online often — and reconcile them with the purchases you've made.
- Report any questionable charges to the card issuer.
- Notify your card issuer if your address changes or if you will be traveling.

MSEFCU is committed to providing you with the most advanced fraud protection solutions available. In keeping with this commitment, we have implemented a tool which allows us to restrict debit card use in countries identified as having a high volume of fraudulent activity.

For more information about fraud prevention and other tips on how to protect your information, visit NCUA Fraud Prevention Center: http://www.mycreditunion.gov/fraud/Pages/default.aspx

**Regulation E: Electronic Fund Transfers**

Regulation E is a consumer protection law designed to protect consumer accounts established primarily for personal, family or household purposes making electronic fund transfers. Excluded from coverage are non-consumer accounts, such as Trust, Corporations, Partnership, etc. The term "electronic fund transfer" (EFT) generally refers to a transaction initiated through an electronic terminal, telephone, computer, or magnetic tape that instructs, or authorizes a financial institution either to credit or debit a consumer's asset account.

Regulation E gives consumers a way to notify their financial institution that an EFT has been made on their account without their permission. If you believe an unauthorized EFT has been made on your account, contact us immediately.

**Non-consumer accounts are not protected by Regulation E.**

A non-consumer member using online banking and/or bill pay is not protected under Regulation E. Because the member is not protected by Regulation E, precautions should be made by the member to evaluate and review the controls in place to ensure that they are correspond with the risk level that the member is willing to accept. The member should also perform a risk assessment and evaluate the controls they have in place periodically. The risk assessment should be used to determine the risk level associated with any internet activities the non-consumer member performs and any controls in place to mitigate these risks.

**Unsolicited Contact**

MSEFCU will never contact its members to request their security logon credentials such as the combination of your username and password. If you receive a request of this type, do not respond to it. Please call us immediately at **800-542-2345 or 209-383-5550** or e-mail us at **info@mercedschoolcu.org** to report any activity of this nature.

MSEFCU will only contact its members regarding online banking activity on an unsolicited basis for the following reasons:

- Suspected fraudulent activity on your account;
- Inactive/dormant account;
- To notify you of a change or disruption in service; or
- To confirm changes submitted to your online banking profile.

If you receive an unsolicited contact from a MSEFCU staff member for any reason not stated above, your identity will be confirmed through a series of security questions and you will always have the option of hanging up and calling MSEFCU to confirm that validity of our request. Remember, we will NEVER ask for your logon security credentials.