Your Rights and Protections Under Regulation E

At MECE Credit Union, your financial security is a top priority. As part of our commitment to transparency and consumer protection, we want to explain the federal protections you have when you use electronic fund transfers (EFTs) on your consumer accounts.

What is Regulation E?

Regulation E is a federal regulation issued by the Consumer Financial Protection Bureau (CFPB) that protects consumers when they make electronic fund transfers. These include:

- ATM transactions
- Debit card purchases
- Direct deposits and automatic withdrawals
- Transfers made through online or mobile banking
- Telephone-initiated transfers
- Person-to-person (P2P) payments

These protections apply only to accounts used for personal, family, or household purposes.

Your Liability for Unauthorized Transfers

If your card, PIN, or online credentials are lost or stolen, your liability for unauthorized transactions depends on how quickly you notify us:

- **Within 2 business days**: Your loss may be limited to $50.
- **After 2 business days but within 60 days** of the statement being sent: You could be liable for up to $500.
- **After 60 days**: You may be liable for the full amount of unauthorized transactions.

To protect yourself, review your statements promptly and report suspicious activity right away.

Error Resolution

If you believe an error has occurred in connection with an electronic fund transfer, contact us immediately. We will investigate and correct any error in accordance with Regulation E. You will receive a written explanation of our findings, and if an error is confirmed, we will make any necessary account adjustments.

Online & Mobile Banking and Regulation E

When you access your consumer accounts through our online or mobile banking platforms, any electronic transfers you make are protected by Regulation E. This includes:

- Bill payments
- Internal transfers between your accounts
- External transfers to or from other financial institutions
- P2P payments from your debit card or account

Please note: **Business accounts are not covered by Regulation E**. Protections for business accounts are defined separately.

Your Responsibilities

To keep your account safe and take full advantage of Regulation E protections:

- Keep your PINs, passwords, and devices secure
- Monitor your account activity regularly
- Report lost or stolen cards or credentials immediately
- Notify us of unauthorized or suspicious activity right away

---

Contact Us

If you have questions or need to report an error or unauthorized transaction, please contact us:

Phone: 573-634-2595
Email: mececu@mececu.com
Secure Message: Log in to Online Banking and send a secure message

---

We Will Never Ask for Your Online Banking Credentials

At MECE Credit Union, protecting your personal and financial information is a top priority. As part of our member education and in alignment with guidance from the Federal Financial Institutions Examination Council (FFIEC), we want to make it clear **under what circumstances, if any, we may contact you and what we will never request from you**.

Unsolicited Requests for Login Information

We will **never** contact you on an unsolicited basis to request your:

- Online or mobile banking username or password
- One-time passcodes (OTPs)
- Debit or credit card PIN
- Full account number or card number
- Social Security number
- Answers to security questions

If you receive a phone call, text message, email, or social media message requesting this type of information—even if it appears to come from [Your Credit Union Name]—**do not respond**. These messages are likely fraudulent attempts to gain access to your account.

How We May Legitimately Contact You

There are times we may reach out to you for valid reasons, such as:

- To verify suspicious activity on your account
- To follow up on a service request or support inquiry you initiated
- To notify you of important account information or security-related updates
- To confirm your identity during an interaction you initiated

In these cases:

- We may ask you to confirm certain **non-sensitive identifying information** (e.g., the last four digits of your account number), but **we will never ask you to disclose or enter your full online credentials** over the phone, by email, or text.
- We will **never pressure you to act immediately**, download software, or click a suspicious link.
- We will encourage you to log in directly through our official website or mobile app, not through a link we send.

Tips to Protect Your Credentials

- **Never share your login credentials**, one-time passcodes, or PINs with anyone.
- **Avoid clicking on links in unsolicited messages** claiming to be from the credit union.
- Always navigate directly to our website: **https://www.mececu.com**
- **Enable two-factor authentication (2FA)** in your account settings for additional protection.
- Regularly monitor your accounts and report any suspicious activity right away.

Report Suspicious Contact

If you believe you have received a suspicious message or phone call, or if you may have accidentally shared your account information, please contact us immediately:

Phone: 573-634-2595
Secure Message: Log in to Online Banking and send us a secure message

Your security is important to us. We will never compromise it—and neither should you.

Protecting Yourself Online: Risk Control Tips and Resources

At MECE Credit Union, we are committed to your financial security. As part of our member education efforts and in accordance with guidance from the **Federal Financial Institutions Examination Council (FFIEC)**, we want to help you understand **practical steps you can take to protect yourself** when using online and mobile banking services.

Whether you're accessing your accounts from home, work, or on the go, these **alternative risk control measures** can help reduce the risk of fraud and identity theft.

✅ Steps You Can Take to Protect Your Accounts

1. **Enable Two-Factor Authentication (2FA)**
   Add an extra layer of protection by requiring a one-time code in addition to your password.
2. **Use Strong, Unique Passwords**
   Avoid using the same password across multiple accounts. Use a mix of letters, numbers, and symbols.
3. **Keep Your Devices Updated**
   Regularly update your computer, smartphone, apps, and antivirus software to patch known vulnerabilities.
4. **Use Secure Networks**
   Avoid accessing your accounts over public Wi-Fi. Use a secure, encrypted connection whenever possible.
5. **Monitor Your Accounts Frequently**
   Review transactions often and report any unauthorized activity immediately.
6. **Be Wary of Phishing Scams**
   Don’t click on suspicious links or attachments in unsolicited emails, texts, or social media messages.
7. **Limit Administrator Access**
   If you use financial software or manage a business account, restrict admin rights to trusted users only.
8. **Use a Password Manager**
   Consider using a trusted password manager to safely store and manage your login credentials.

📚 Helpful Resources for Online Security

To stay informed on emerging cyber threats and best practices for protecting your information, we recommend the following trusted sources:

- **StaySafeOnline (National Cybersecurity Alliance):**
  https://staysafeonline.org
  Offers consumer-friendly guidance on passwords, mobile device security, and phishing awareness.
- **Federal Trade Commission (FTC):**
  https://www.consumer.ftc.gov
  Includes helpful information on identity theft, scams, and data privacy tips.
- **Cybersecurity & Infrastructure Security Agency (CISA):**
  https://www.cisa.gov
  Provides alerts, toolkits, and advice for securing systems and devices.
- **FDIC Consumer News:**
  https://www.fdic.gov/resources/consumers/consumer-news/
  Shares practical tips on banking securely and avoiding common fraud schemes.

🔒 We're Here to Help

If you'd like help setting up security features on your account or learning more about how to stay safe online, contact us:

Phone: 573-634-2595
Secure Message: Log in to Online Banking

Your role in protecting your financial information is essential—and we're here to support you every step of the way.

Report Suspicious Activity or Security Concerns

If you notice **unusual activity** on your account or believe your personal or financial information has been compromised, **contact us immediately**. Quick action is the best way to protect your accounts and limit potential losses.

In accordance with **FFIEC member education guidelines**, we are providing the following contact options for your use at any time.

🔎 **Contact Options for Security-Related Issues**

📞 **By Phone (Immediate Assistance):**
Call our Member Services Team at **573-634-2595**
Available: **8:00 am – 4:30 pm CST, Monday - Friday**
If it's after hours, follow the phone prompts for lost or stolen cards or urgent fraud reporting.

💬 **Secure Online Message:**
Log in to Online Banking or the Mobile App and send us a secure message describing the issue.

📧 **By Email (Non-Urgent Inquiries Only):**
Email us at **mececu@mececu.com**
(Please do not include confidential account information in unsecured emails.)

🏢 **In Person:**
Visit us at 2722 E. McCarty, Jefferson City, MO 65101 to speak with a representative.

📄 **Lost or Stolen Card?**
Call: (888) 297-3416
Or use your mobile app to disable the card temporarily.

🚨 **Examples of When to Contact Us**

- You see suspicious transactions on your account
- You've received a phishing email, phone call, or text message claiming to be from us
- Your debit or credit card has been lost or stolen

- You believe someone has gained unauthorized access to your account
- You've accidentally shared personal information (e.g., passwords or account numbers)

📱 Mobile Banking Threats to Watch For

Mobile banking is convenient, but it also comes with risks. Be alert for:

- Malicious apps that mimic legitimate banking apps—only download from trusted app stores
- Smishing (SMS phishing): Fraudulent text messages that ask you to click on links or enter login info
- Fake phone calls or voicemails pretending to be from the credit union
- Unsecured public Wi-Fi used to access banking apps or sites
- Device theft where a stolen phone may give access to saved passwords or apps
- Outdated operating systems or apps that may contain security vulnerabilities

How to stay safe:

- Use biometric or PIN protection on your mobile device
- Keep your device's operating system and banking app up to date
- Use official app stores and avoid third-party download sites
- Never respond to texts or messages asking for account details or passcodes
- Enable remote wipe or tracking features in case your device is lost or stolen

🛡️ We're Here to Help

Your security is our priority. If you're unsure whether something is legitimate or need guidance on how to respond to a possible scam or data breach, **don't hesitate to reach out**. We're here to assist you with fraud prevention, detection, and recovery.