

EWWEB

EMPLOYEES

Federal Credit Union

Fall 2017

September 2017



New Website and Online Banking will launch early October along with our new core data processor!

We are pleased to partner with a US based core data processor. We are also excited about the new features available for our home banking users!

New features include single sign on to access online banking, bill pay, e-statements, e-notices, e-receipts and finally - remote deposit capture!

As we convert to the new service providers it will be necessary to re-enroll in online banking with your first login into the new website. You will also need to set up your bill pay payables again.

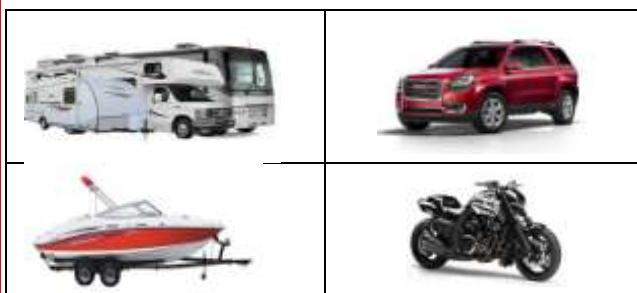
Credit Union staff will be available to help you each step of the way to get everyone back up and running. We apologize for the disruption but trust that the new features will be worth the extra trouble of new set ups. Thank you for your patience as we learn new systems.



We have a full line of mortgage products available for purchase, refinance and home equity.

- Fixed rate terms up to 30 years
- Low Closing Costs
- Loans are held in house and we service them ourselves
- Many times an appraisal is not needed

Equal Housing Lender / Mortgage Lender #743128



Yes, we have loans!

New or Used, Purchase, Refinance or Cash Out to take care of other expenses. We have great rates and very quick turnaround time.

Come see us or give us a call to get started.



Holiday Closings
 Veterans Day - Friday, November 10th, 2017
 Thanksgiving - Thursday and Friday, November 23rd, 24th, 2017
 Christmas - Monday, December 25, 2017
 New Years - Monday, January 1, 2017



Roberta Nelson Memorial Scholarship Winner

We are pleased to announce the winner of this year's Roberta Nelson Scholarship award of \$1,000 went to Hannah Morse. Hannah will be attending Pacific University majoring in pre-med. Best of luck to Hannah in her studies!

We'd like to express our appreciation to all of you who bought Roberta Nelson Memorial Scholarship raffle tickets at the Annual Meeting.

Thanks to those of you who contribute all year long toward the fund when you visit our office. Don't forget: you can set up a payroll deduction from your paycheck or automatic transfers toward this fund--it's easy and tax-deductible, too!

Senior Safety and Account Review

As a reminder to our member's, it's never too often to check your account structure's with all of your financial institutions.

Make sure beneficiaries and joint owners are up to date. Think about setting up a power of attorney prior to the emergencies when you might need them.

Come down to the credit union for an account review today.



*Skip a Payment
for the Holidays!*

Every year the Credit Union offers members an opportunity to skip a loan payment in November, December, or January. We know that expenses can go up during the holiday season, and this payment skip can help make the season more affordable.

Visa credit cards, real estate loans, lines of credit and some auto loans do not qualify for the skip payment special. Interest will continue to accrue on the outstanding balance. \$25 fee applies.



63rd Annual Meeting and Picnic

The 63rd Annual Meeting and EWEB All Family Picnic was held on August 5, 2017 at Lloyd Knox Park cosponsored by EWEB, EWEB Retirees and EWEB Credit Union.

We counted over 185 in attendance ranging in ages from infants to seniors. It appeared that a good time was had by all. We had good food, conversation and games. The weather cooperated with sunshine and moderate temperatures.

Two Board Members were reelected for another term. They were Mary Beckman and Jim Origliosso.

Thank you to all the volunteers who made this event a success, we look forward to next year.



ATM LOCATOR

EWEB Employees Federal Credit Union Members who have our debit card receive unlimited access to their EWEB EFCU checking and savings at our ATM's to withdraw funds or make transfers. Plus, access cash surcharge free where ever you are nationwide with the credit-union owned Co-Op network ATM's.

Our website has a link to the Co-Op ATM Locator website (www.co-opnetwork.org). If you are planning on traveling or just want to find an ATM location which is on the Co-Op Network click on the Co-Op logo on the bottom of the page. Co-Op has over 28,000 ATM's nationwide with 5,500 located in 7-11 store locations.



Regulation D FAQs

- What is Regulation D?
- What transactions are not affected by Regulation D?
- What are my options once an account has reached its Regulation D limit?
- If an account used for Overdraft Protection has reached its Regulation D limit, will overdraft requests be honored?
- I have authorized a merchant to automatically withdraw payments from my Savings Account or MMA; do these count against my monthly limit?

What is Regulation D?

Federal Regulation D places a **monthly** limit on the number of transfers you may make from your **Savings Accounts** or **Money Market Accounts** (MMAs) without your physical presence being required. Transfers affected by this regulation therefore include:

- Transfers made using Online Banking.
- Transfers made using Telephone Banking.
- Overdraft transfers (made automatically to cover insufficient funds in other accounts; see below).
- Transfers made by a Member Service Representative on your behalf.
- Pre-authorized, automatic, scheduled or recurring transfers (see below).

You are allowed **six such transfers per month**, per account before a \$5 fee per transaction is assessed.

What transactions are not affected by Regulation D?

- ATM transactions.
- Transfers made to EWEB EFCU loans.
- Transactions done in person at the branch.
- Transactions sent in by mail or Night Drop with an original signature.
- EWEB EFCU Bill Pay (which uses funds from your checking account).

What are my options once an account has reached its Regulation D limit?

You may complete withdrawals and transfers in person, by mail or at an ATM.

If an account used for Overdraft Protection has reached its Regulation D limit, will overdraft requests be honored?

Yes, if the Overdraft Protection account is a Savings Account. In that case, you will receive a notice by mail and be assessed the \$5 for every overdraft attempted beyond your monthly limit. However, if the Overdraft Protection account is a Line-of-Credit loan (which is not affected by Regulation D) the overdraft will complete normally. To apply for a Line-of-Credit loan, apply online or contact us.

I have authorized a merchant to automatically withdraw payments from my Savings Account or MMA; do these count against my monthly limit?

Yes. These payments (which you might know as “ACH” or “EFT” transactions) follow Regulation D limitations. Any withdrawals attempted beyond your monthly limit will be assessed the \$5 fee. To avoid this situation, make automatic payments using something other than a Savings Account or MMA, such as a checking account. Contact the merchant to arrange this change, and be aware that your request could take more than a month to go into effect. Alternatively, consider using EWEB EFCU Bill Pay to automatically send payments to the merchant, rather than authorizing the merchant to automatically withdraw payments.



PO Box 12000 Phone: (541) 484-5304
Eugene, OR 97440 (800) 796-3756
Fax: (541) 345-5834
388 Pearl St, Suite 1 Hours: M-F 9 am – 5 pm
Eugene, OR 97401
Email: ewebcu@myewebcu.org
Editor: Rose Staggenborg

Equal Housing Lender

10 tips to prevent ID fraud during the holiday season

Identity fraud can happen to anyone at any time. However, there are simple steps you can take to reduce your risk and make it more difficult for criminals to steal and commit fraud with your personal information. Joe Reynolds, Identity Fraud Product Manager from Travelers, offers these 10 tips.

Traditional Shopping: Before Black Friday and Beyond

1. Review your wallet or purse contents before you go shopping

Common theft is the easiest way for a criminal to steal your identity and commit fraud. Avoid carrying Social Security cards, birth certificates or passports unless absolutely necessary. Don't carry extra credit cards unless you plan to use them.

2. Create a list of all your credit card and bank account information and store in a secure place

Be sure to include account numbers, expiration dates and credit limits. Also include the telephone numbers of the customer service and fraud departments. If you find your card missing or stolen, refer to this list and immediately notify your credit card provider of the loss. This not only prevents fraudulent charges, but it also notifies your provider if the card is used again.

3. Protect your Passwords and PINS

When creating passwords and PINs, do not use the last four digits of your Social Security number, mother's maiden name, your birth date, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves. It's best to create passwords that combine letters and numbers. Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code or password -- a number or word -- when accessing your account. Memorize all your passwords. Don't record them on anything in your wallet.

4. Review your credit report now -- and after the New Year

One of the easiest ways to see if a criminal is fraudulently using your identity is to review your credit report. Be sure to report mistakes to the credit bureaus. A federal law gives consumers the right to receive one free copy of their credit report every 12 months from each of the three main credit bureaus (Experian, Equifax, TransUnion). Order a report today from one bureau and review it, looking for discrepancies. A couple months after the New Year, order another report from a second bureau. Four months later, order a report from the third bureau. Doing this will enable you to see snapshots of your credit throughout the year at no cost.

5. Never provide confidential information over the phone to an unsolicited caller claiming that they represent a financial institution or creditor

Criminals often will use your social security number to open up fraudulent accounts or gain access to financial information or assets, especially with increased activity around the holidays. Do not have your Social Security Number printed on your checks and do not allow merchants to write your SSN on your checks. If a business requests your SSN, ask them why they need it. If it is not a valid reason, don't provide it. If you receive an unsolicited call and are asked to provide information, get the caller's name, location, telephone number, and reason that they are calling. Call them back at the phone number on your billing statements to verify the caller's identification.

6. Never put outgoing checks or bill payments in your home mailbox

While sending checks is a popular and desired holiday gift, it also has its risks. Thieves can steal mail containing checks and gain other personal information from bills and financial statements. Where practical, drop all items containing checks or financial information in a secure postal mailbox or at the post office.

Online Shopping: Cyber Monday and Beyond

7. Log off completely when finished with online transactions

Closing or minimizing your browser or typing a new Web address may not be enough to prevent others from accessing your online information. Instead, click 'log off' to terminate your online session. In addition, don't allow your browser to "remember" your username and password information.

8. Increase your own computer's security

Personal firewalls and security software packages -- with anti-virus, anti-spam, and spyware detection features -- are a must-have for those who plan on shopping online this season. Make sure your computer has the latest security patches, and make sure that you access your online financial accounts only on a secure online page using encryption.

9. Avoid e-mailing personal and financial information

Although your computer may be 'well protected' with proper firewall, antivirus, Internet security or encryption software, the individual or company receiving your information may not have similar security in place. Always confirm with online retailers that they have proper Internet security in place before responding to any e-mail request.

10. Delete, without replying to, any suspicious e-mail requests

Hackers and spammers often impersonate retailers to lure personal financial information. If there is any reason to doubt the authenticity of an e-mail message from a company you do business with, don't click on links or buttons in the message. Instead, type the Internet address of the company into your browser, log on as you usually do, and examine your account information. You may also telephone a company to ask if an e-mail is legitimate.