How to Safeguard your Information

At Linn-Co Federal Credit Union, the security of member information is a priority. We are strongly committed to the safety and confidentiality of your records. One of the best ways to avoid becoming a victim of identity theft or other kinds of fraud is to become an educated consumer. Please take a moment to read this important information on how to keep your information safe.

What is Identity Theft?

Identity theft involves the unlawful acquisition and use of someone's identifying information, such as:

- Name
- Address
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Driver's License
- Credit Union, Bank or Credit/Debit Card Account Number

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity, which may include opening new accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

Fraudsters will use a variety of methods to obtain your information: regular mail, e-mail (phishing), text messages (smishing), telephones (vishing) or spoof websites. Don't respond to requests for personal or financial information. Delete the email or text, discard the letter or simply hang up the phone.

How do I protect myself?

- Report lost or stolen checks or credit cards immediately
- Never give out any personal information, including birth date, SSN or passwords
- Secure any documents containing personal information
- Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices

Protecting Yourself Online

1. **Set good passwords.** A good password is a combination of upper and lower case letters, numbers and symbols and one that is not easily guessed. Don't use personal information, such as dates of birth or social security numbers in your password. Change your password frequently. Don't write it down or share it with others.

2. **Don't reveal personal information via e-mail.** Emails and text messages can be masked to look like they're coming from a trusted sender when they're actually from someone else. Play it safe. Do not e-mail or text personal information, such as account numbers, social security numbers, passwords, etc.

3. **Don't download that file!** Opening files attached to emails can be dangerous, especially when they're from someone you don't know. They can allow harmful malware or viruses to be downloaded onto your computer. Make sure you have a good antivirus program on your computer and that it's up to date.

4. **Links aren't always what they seem.** Never login from a link that is embedded in an e-mail address. Criminals can use fake email addresses and make fake web pages that mimic the page you would expect. To avoid falling into their trap, don't click on the link in the e-mail. Type the URL address directly into your browser and then log in.

5. **Websites aren't always what they seem.** Be aware that if you navigate to a website from a link and not from a URL address you've typed in directly. You may end up at a site that looks like the correct on, when, in fact, it's not. Take time to verify that the web page you're visiting matches exactly with the URL you'd expect. Also, don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it. Look for https:// and a lock symbol in the URL address to determine if the website is secure.

6. **Avoid using public computers to access your online banking.** And be sure to log off properly when finished with your online banking session, rather than just closing the page. Does the page have a Log Off button? Use it!

7. **Monitor account activity.** Review your account activity regularly, either online or by reviewing your periodic statements. Report any unauthorized transactions right away, by calling 541.259.1235 and talking with a Member Service Representative.

Online Banking Security

Linn-Co is committed to protecting your personal information. 24-7 Click uses several different methods to protect your information. All information within our online banking uses the Secure Socket Layer (SSL) protocol for transferring data. SSL creates a secure environment for the information being transferred between your browser and Linn-Co. All information transferred through 24-7 Click has a 128-bit encryption.

Debit Card Protection

Debit card usage has increased dramatically in recent years and fraudulent use of debit cards has also increased. Here are some suggestions on the care and usage of debit cards.

- Treat your debit card as you would cash. Always keep plastic cards in a safe and secure place.
- Do not send your card number through an email.
- Do not give out your card number over the phone, unless you initiated the call.
- Regularly review your account statements and contact the credit union immediately, if you notice any discrepancies.
- Don't give out your PIN or write your PIN down, especially on the card. Memorize it.
- Make sure any internet purchase is secured with encryption to protect your account information. Look for https:// and a lock symbol in the URL address to determine if the website is secure.

Regulation E: Electronic Fund Transfers

The Federal government has put in place rights and responsibilities for both you and the credit union, regarding electronic transaction activity. Regulation E defines these rights, responsibilities and liabilities and is described in the Account Agreement you received when you opened your account with Linn-Co. If you notice suspicious or unauthorized account activity or experience security-related events, please contact the credit union at 541.259.1235. After-hours help is available for credit card members at 800.808.7230 and debit card members at 800.554.8969.

Mobile Banking Security

Browsing the web has never been easier – it's all at your fingertips. Smartphones let you surf, shop or bank wherever you are. Make sure your information stays secure while you're on the move by following these smartphone-safe browsing tips:

- Activate your phone's password feature, which locks the screen and prevents anyone but you from accessing your phone. Set up the password feature on your phone with a code that only you know.
- Don't connect to unknown networks through Wi-Fi hotspots to make financial transactions.
- Beware of smishing – Attempts to obtain personal information on phones through text messages. Never download media or images, or click on text-message links that come from unrecognizable people or phone numbers. Never provide personal details or any account details using any form of electronic messaging because this is not a secure form of communication.
- Download apps exclusively from the official source for your smartphone's platform, such as the Android, Apple or BlackBerry stores.
- Install anti-virus software for your smartphone when available and update it frequently.
- Install location finding applications, which work with your phone's built-in GPS. These applications allow you to locate and/or remotely erase (or "wipe") data in your phone if it is lost or stolen.
- Update your smartphone's operating system as soon as newer versions are available.
- It's convenient to have apps remember login credentials. However, it's a bad idea to have them remember your banking or other financial institution credentials. Take the extra effort to log in every time.
- If you lose your phone, disable the phone through the 24-7 Click Self-Service tab or contact us at 541.259.1235 for assistance.
- Maintain mobile deposit items in a secure location. After reconcilement, dispose of the documents by shredding or otherwise destroying the item.

Important Information for Business Members

It is critical that business members implement sound security practices within their places of business as outlined in this document to reduce the risk of fraud and unauthorized transactions from occurring.

We recommend periodically assessing your online banking risk and network security. You should put in increased security controls where weaknesses are found. Some items to consider when assessing risk are:

- Who has access to your online business accounts?
- How and where are user names and passwords stored?
- How strong are your passwords and how often are they changed? Are they changed before or immediately after terminating an employee who had access to them?

- Do you have dual controls or other checks and balances with respect to access to online banking transactions?

Corporate Account Takeover is a form of identity theft in which criminals steal your valid online banking credentials. The attacks are usually stealthy and quiet. Malware introduced onto your systems may go undetected for weeks or months. Account-draining transfers using stolen credentials may happen at any time and may go unnoticed depending on the frequency of your account monitoring efforts.

Here are some ways to protect your company:

- Use layered system security measures: Create layers of firewalls, anti-malware software and encryption. Keep the programs updated.
- Educate your employees about cybercrimes. Make sure your employees understand that just one infected computer can lead to an account takeover.
- Block access to unnecessary or high-risk websites. Prevent access to any website that features adult entertainment, online gaming, social networking and personal e-mail. Such sites could inject malware into your network.
- Establish a separate user account for every employee accessing financial information and limit administrative rights for those users.
- Use approval tools in cash management to create dual control on payments. Requiring two people to issue a payment doubles the chances of stopping a criminal from draining your account.
- Review or reconcile accounts online daily. The sooner you find suspicious transactions, the sooner the theft can be investigated.

What to expect from Linn-Co FCU

- Linn-Co will *never* call, e-mail or otherwise contact you and ask for your user name, password or other online banking credentials.
- Linn-Co will *never* contact you and ask for your credit or debit card number, PIN or 3-digit security code.
- The credit union or a contracted 3rd party card service provider may contact you regarding a potentially suspicious transaction.
- If contacted by the credit union or a contracted 3rd party card service provider, they may ask to verify your street address, the last 4 digits of your social security number, the last 4 digits of your card number or the amount of your last transaction. They will *never* ask for your card number, expiration date or 3-digit security code.
- If you're uncomfortable with the call, please hang up and call the credit union at 541.259.1235.

Additional Resources

The following links are provided as a convenience to our members. Linn-Co neither endorses nor guarantees, in any way, the organizations, services or advice associated with these links. Linn-Co is not responsible for the accuracy of the content found on these sites.

- Learn how to secure your computer, avoid internet fraud and protect your personal information: www.onguardonline.gov
- Identity Theft, Privacy, and Security Publications for Businesses www.business.ftc.gov/privacy-and-security
- Consumer information from the FTC: www.consumer.ftc.gov
- Oregon Department of Justice Consumer Protection: www.doj.state.or.us/consumer
- Experian Credit Bureau: www.experian.com 1.888.397.3742
- Transunion Credit Bureau: www.transunion.com 1.800.680.7289
- Equifax Credit Bureau: www.equifax.com 1.800.525.6285