Do not let the Equifax cybersecurity incident affect you.

Ocala Community Credit Union recommends our members follow a few everyday preventive steps to secure their identity.

Strengthen Your Digital Security

- Use strong passwords and PINs. Your passwords and PINs shouldn't be something anyone could guess, even if they had access to some of your personal information. Avoid names, addresses, and important dates.
- Keep passwords and PINs safe. Never store passwords or sensitive information unencrypted on your computer. If you have a physical "cheat sheet" of log-in information, keep it locked up.
- Protect your computer. Identity thieves use complex software such as spyware and key loggers to obtain sensitive information. A strong and regularly updated firewall, anti-virus program, and anti-spyware program will provide most of the protection you need.
- Beware of phishing scams. You may receive a seemingly harmless email asking you to verify certain things such as your password, account number, or personal identification information. Any email seeking this sort of information should be an immediate red flag for you. The best response is to contact the service provider directly and ask what's up. DO NOT CLICK ON ANY LINKS IN AN EMAIL YOU'RE UNSURE OF.
- If getting rid of an old computer, laptop, cell phone, or table-Restore old computers to factory settings. Whether you're selling an old computer, recycling it, or throwing it away, make sure you dispose of it safely. Restoring it to factory settings ensures all of your information is gone.

Enhancing Home Security

- Shred sensitive documents. Old billing statements or any other documents that contain any personally identifying information (even if it's just your name and address) these documents shouldn't be thrown away in the regular trash.
- Opt out of pre-screened credit offers. Many thieves will use offers to apply for credit in your name at a different address, or will try to use cash advance checks. You can eliminate this opportunity and help prevent identity theft by calling the opt-out number to stop receiving credit card offers.
- Keep valuable documents locked away. Personal documents related to your identity, such as your Social Security or national insurance card, birth certificate, and passport, should ideally be stored in a locked, fireproof safe.
- Avoid broadcasting personal information. Even when you're at home, you still need to be cautious when discussing sensitive matters over the phone. This is particularly true if you live in a densely populated area.

Staying Alert Out in Public

- Watch out for "shoulder surfers." That person behind you in line at the ATM or the supermarket may just be another shopper, or they could be paying close attention to you in hopes of seeing your account balance or PIN.
- Carry only what you need. There typically is a lot of identifying information in your wallet or handbag. If stolen, the person can use that information to steal your identity. For your protection and to help prevent identity theft, leave anything at home that you aren't planning on using.
- Avoid using insecure public Wi-Fi networks. If you're out and about, it can be convenient to take advantage of the free public Wi-Fi available at many cafés, libraries, airports, and public parks. However, if these networks are open to all, they come with risks.
- Use only ATMs with adequate security. If you want to get cash with your debit card, you should use an ATM located inside a bank branch – even if you have to go a little out of your way. Private ATM machines, particularly those outdoors, present a tremendous risk.

Minimizing the Damage of Identity Theft

- Contact your financial institutions and credit card companies. If you believe someone has stolen your identity, or if your wallet or handbag is lost or stolen, call every bank or credit card company potentially implicated as quickly as possible to get your cards cancelled.
- Keep a list of these phone numbers at home in case of a lost or stolen wallet, as usually the phone numbers are located on the card.
- Put a fraud alert on your credit report. In the United States, a fraud alert requires any creditors to take additional steps to verify your identity before issuing any credit in your name.
- Change all passwords. As soon as you have reason to believe your identity may have been stolen, take precautions to minimize the damage and change passwords for everything, regardless of whether they contain any sensitive information.
- Order copies of your credit report. If you're concerned your identity might have been stolen, review your credit report and note any suspicious transactions or entries, such as requests for credit in your name or new cards for which you never applied.
- File a complaint with the Federal Trade Commission (FTC). The FTC operates a Complaint Assistant website that will guide you step-by-step through the process of filing an identity theft complaint. You will need this complaint to prove your identity was stolen.
- File a police report. In addition to filing an FTC complaint, you also need to file a report with your local police precinct (or the precinct where the theft occurred, if you're traveling). Call the non-emergency number and tell the operator you wish to file a police report for identity theft.
- Maintain complete records. While you're dealing with the aftermath of identity theft, keep detailed notes of everyone you contact and everything that is said. Send follow-up letters confirming phone conversations so everything is in writing.

Again, please don't hesitate to contact us with any questions or concerns.