

# Identity theft

- ✓ Keep confidential information private
- ✓ Monitor your accounts
- ✓ Sign up for eStatements

Protecting your confidential information will help you avoid identity theft.

Identity thieves want confidential information, such as your Social Security Number, credit card numbers, passwords, or your mother's maiden name. They usually get their information from you. Here are some ways they may try to pry into your life:

- **Internet** – Fraudulent, but official-looking emails or pop-up windows that ask you to update information or enter a contest.
- **Mail** – Theft from your mailbox or trash.
- **Phone** – Calls to "verify" information.
- **Text messaging** – Messages delivered directly to your cell phone threatening account closure.
- **ATMs and Point-of-Sale keypads** – Someone watching over your shoulder.

## How Alaska USA protects your information

- Alaska USA will never call, email, or text you asking for your account information. When you call the credit union, you will be asked questions to verify your identity.
- Alaska USA has the latest in Secure Sockets Layer (SSL) technology to protect your information when you access UltraBranch® online, and your session ends automatically after 10 minutes of inactivity.
- Your Alaska USA Visa® credit and check card are monitored for suspicious or unusual activity. Call the Member Service Center to update your contact information, if you plan to travel overseas, or if you intend to use your card in a way that's unusual for you.

## Ways to protect your information

- **Be a savvy tech user** – Change your UltraBranch password periodically and keep it secure. Do not store passwords on

your computer, as these are susceptible to keystroke loggers and malware exploitation.

Install and update firewall, anti-spyware, and anti-virus software on your computer.

Don't click on links in emails you receive. Instead, call the company or access to their website directly.

Avoid emailing confidential and financial information and never share it on a social media site (e.g. Facebook, MySpace, etc.).

Sign up to receive your account statement electronically with eStatements, and keep your account information out of the wrong hands.

- **Regularly monitor your accounts** – Use UltraBranch online or by phone, and set email alerts for low account balances
- Review your credit card and account statements as soon as you receive them to watch for any irregularities.

Check your credit report annually. Order yours free at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling (877) 322-8228.

- **Use your memory, and your shredder** – Shred account statements, bills, preapproved credit offers, and other personal documents before you toss them.

Memorize your PIN for your Alaska USA ATM or Visa check card. Never write your PIN on your ATM card, carry it in your wallet, or file it in an obvious place.

- **Additional security** – Sign up for Verified by Visa, an added safeguard when you use your Alaska USA Visa check or credit card for online shopping. Find out more under credit cards [atalaskausa.org](http://atalaskausa.org).

Put a password on your account to be used when calling the Member Service Center.

## Learn more

You can download helpful publications and find out more about identity theft at [www.IdentityTheft.gov](http://www.IdentityTheft.gov).

## Protect yourself

Identity thieves aren't always strangers! You can do a lot to protect yourself if you keep your confidential information private. Don't give out your passwords or Personal Identification Numbers (PINs); never write them down and leave them in plain view.

## Sound the alarm

If you believe there are unauthorized transactions on any of your Alaska USA accounts, call the Member Service Center immediately.

[alaskausa.org](http://alaskausa.org)

**NCUA**

Federally insured by NCUA

**AlaskaUSA**<sup>®</sup>

AKUSA 02495-1 0515 - AK