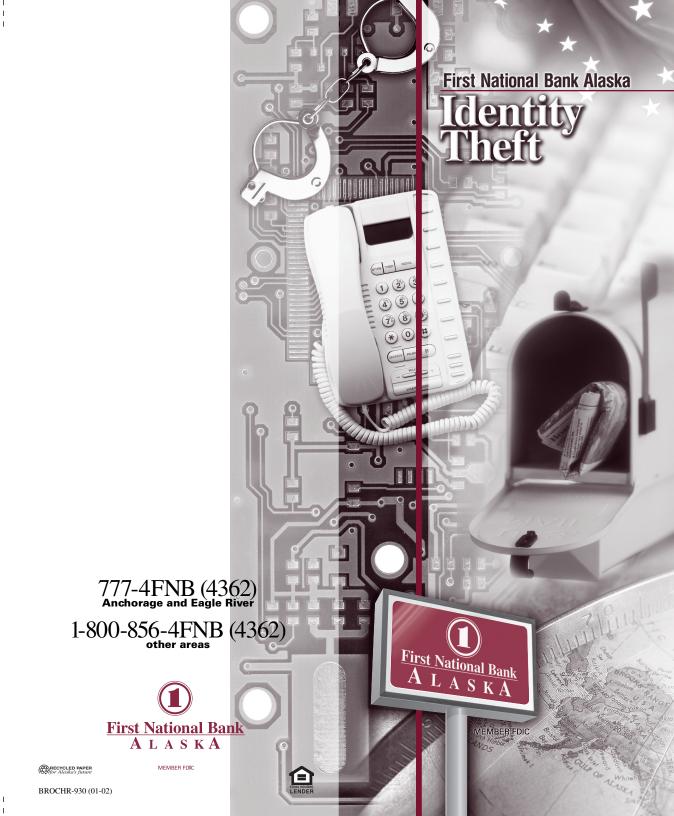


At its simplest level, identity theft is someone pretending to be you. A typical identity thief might, for example, use personal information such as your address, phone number and/or social security number to open a fraudulent credit card account in your name. The concept is simple, but over the last 10 to 15 years it has been used in increasingly sophisticated ways to defraud honest and unsuspecting individuals.





How do identity thieves get my personal information?

To get your personal information, an identify thief might:

- · Steal your wallet or purse.
- · Steal your mail.
- Find your personal information in your home.
- Divert your mail to another location by filling out a "change of address" form.
- · Rummage through your trash, at home or work.
- Get a copy of your credit report by pretending to be your landlord or employer.
- Get the information from a third party (by paying a store employee, for example, to obtain information you put on a credit card application).

What does an identity thief do with the information?

Common schemes involve:

- Opening a credit card account using your name, date of birth and social security number.
- Calling your credit card issuer and, pretending to be you, asking to change the mailing address on your account. The imposter then runs up charges on your account. Because the bills are sent to the new address, it may be some time before you realize there's a problem.
- Establishing phone or wireless service in your name.
- Opening a bank account in your name and writing bad checks.
- Filing for bankruptcy under your name to avoid paying debts they've incurred, or to avoid eviction.
- Counterfeiting your checks or debit cards, and draining your bank account.
- Buying cars by taking out auto loans in your name.

How can I protect myself from identity theft?

The key to protecting yourself is managing your personal information carefully.

- Think carefully before giving out personal information. Ask the other party how the information will be used.
- Pay close attention to your billing cycles. Contact creditors if their bills don't arrive on time.
- Check account statements carefully.
 Make sure all charges, checks and withdrawals were authorized.
- Store personal information in a safe place. Tear up charge receipts, insurance forms, credit card offers and other such documents before you throw them away.
- Guard your mail against theft.
 Promptly remove mail from your mailbox after it has been delivered.
- Deposit bill payments in a locked collection box or at a post office.
 Don't leave them in your mailbox, where they might be stolen.
- Let the U.S. Postal Service (1-800-275-8777) know when you will be on vacation. Request that they hold your mail until you return.
- Protect your accounts with passwords and PINs identity thieves can't easily guess. Avoid using easily available information such as your name or birth date.

(TIP: THINK OF A FAVORITE SONG. USE AS YOUR PASSWORD THE FIRST LETTER OF EACH OF THE FIRST TEN WORDS TO THE SONG.)

• **Lighten your load.** Carry only the minimum amount of identifying information and number of credit cards that you need.

I think someone is stealing my identity. What should I do?

If you suspect someone is using your identity:

 Contact the Federal Trade Commission (FTC). Their booklet, "ID Theft: When Bad Things Happen To Your Good Name," is a comprehensive identity theft reference guide. In simple, easy-to-read language, it spells out your rights and responsibilities and provides instructions on what to do and who to contact.

Obtain a copy of the booklet by calling the FTC toll-free at 1-877-IDTHEFT, or by writing them at:

Federal Trade Commission Identity Theft Clearinghouse 600 Pennsylvania Ave NW Washington D.C. 20580

The booklet can also be found online at http://www.consumer.gov/idtheft (if you don't have a computer, you may be able to obtain online access at your local library).

2. Contact the fraud department of each of the three major credit bureaus. Explain the situation and ask them to add to your file both a "fraud alert" and a statement instructing creditors to call you before opening or changing any accounts.

- 3. Contact the security or fraud departments of your creditors. Explain the situation, and have them close accounts that identity thieves have used. Call your creditors as soon as possible, but always send a follow-up letter as well, and keep a copy for yourself (it is important to establish a "paper trail" for investigators).
- 4. **Call the police.** Be sure to get a copy of the police report for your records.