# Keep your good name.

Refuse to be a target of identity crime.

## Protect Yourself from Identity Crime

If you have been the victim of identity crime, you might not know it until you have been denied credit, received a bill for something you did not buy, or received a credit card for which you did not apply. It can take months or even years to repair your credit and restore your good name after someone has used your identity. Take steps now to protect yourself from identity crime.

### What Is Personal Identifying Information?

- Name
- Address
- Date of birth
- Social security number
- Telephone numbers
- Driver's license number
- Account numbers
- Passwords
- PIN numbers
- E-mail address and screen name

### How Do Criminals Get My Personal Identifying Information?

- Steal your wallet or purse
- Burglarize your home
- Steal your credit or debit card numbers
- Steal mail from your mailbox
- Go through your trash
- Fraudulently obtain your credit reports or personnel records
- Divert your mail using a change-of-address form
- Ask you to give your account numbers over the phone or by e-mail
- Purchase information from unscrupulous employees at companies with which you do business
- Burglarize businesses that have your information on file
- Hack into your computer

### What Do Criminals Do With My Personal Identifying Information?

- Make purchases with your credit cards, sometimes after calling the card issuer and asking for a change of mailing address to divert bills and delay detection.
- Drain your bank account using electronic fund transfers, counterfeit checks, or a debit card.
- Open a new credit card account in your name.
- Establish utility, telephone, or Internet service in your name.
- Open a bank account in your name and write bad checks on that account.
- File for bankruptcy in your name to avoid paying debts they have incurred in your name.
- Buy cars in your name.
- Give your name to police after an arrest.
- Use your name and credit when they buy goods and services to be used in illegal activities.
- Use your social security number to obtain employment.

### What Is Identity Crime?

Identity crime is the illegal use of another's personal information, such as credit card numbers, social security number, or driver's license number to commit fraud or other crimes.

One in four people will be impacted by the fastest growing crime in America, IDENTITY CRIME.

For more information about identity crime, visit www.idsafety.org.

In partnership with:

Bank of America

**How Can I Protect My Identifying Information?**

Safeguard your social security number:

- Remove your social security number from your driver's license, personal checks, and financial documents.
- Store your social security card in a safe place in your home, such as a locked safe, not in your purse or wallet.
- Write to any businesses or institutions that use your social security number as your identification number and ask them to issue different identification numbers for you.
- Give your social security number only to those parties that have a legitimate need for it, such as financial institutions or employers who require your social security number for wage and tax reporting purposes.
- Give your social security number only to those private businesses with which you have initiated contact and those that give satisfactory answers to the following questions:

  Why do you need my social security number?

  How will you use it?

  How will you protect it from being stolen?

  What will happen if I do not give it to you?
- Ask your employer about the security of your social security number and other personal identification information at work, and verify that access to your personal information is restricted to those who need access and that the records are kept in a secure location.

Safeguard your credit cards and personal checks:

- Keep your wallet or purse in a secure place at all times.
- Carry only one or two credit cards in your wallet or purse, and store any others in a secure place.
- If your passwords are written down somewhere, store those records separately from your credit cards.
- Password-protect all credit card accounts that allow it.
- Choose passwords and personal identification numbers that would be difficult for someone who knows you to guess, and avoid such popular ones as birth dates, house numbers, a spouse's name, or mother's maiden name.
- Arrange to pick up new checks at your bank rather than have boxes of new checks delivered to your home, where postal carriers might leave the oversized boxes on your doorstep.

Safeguard your personal papers:

- Keep credit account information in a safe place, such as a locked safe.
- Always ask for a receipt when you pay with a credit or debit card, and take your receipts home with you for shredding.
- Get in the habit of shredding all personal or financial documents before placing them in the trash. Shred copies of bills and invoices after you have paid them, bank statements (including your cancelled checks), investment or retirement account statements, preapproved credit card or loan applications (especially those that come with a negotiable check attached), medical statements of any kind, and any other documents with information about you or your finances.

Safeguard your mail:

- Install a locked mailbox or front-door mail slot at your home or use a post office box to receive mail.
- Send mail, especially payments, from a curbside public mailbox or from the local post office.
- Remove your mail promptly from your mailbox.
- Never leave outgoing mail in an unsecured mailbox overnight.
- Ask the post office to hold your mail while you are away from home for any length of time by calling 800.275.8777, or visit www.usps.gov.

Protect your information on the phone and on the computer:

- When placing an order on the phone or online, use a credit card rather than a debit card.
- Give credit account information over the phone only if you initiated the call and know the business.
- Remember that banks, credit card companies, telephone companies, and other legitimate creditors do not call to verify account numbers or to ask for your social security number or other personal information.

**How Can I Protect My Identifying Information? (cont'd.)**

Protect your computer:

- Assume that any e-mail or pop-up messages on your computer that claim that there is a problem with one of your accounts is fraudulent, and call the company or institution with which you have the account to verify that there is no problem and to report the attempted fraud.
- Install virus and spyware detection software and update it regularly.
- Avoid opening e-mail messages or attachments or following hyperlinks that you receive from strangers.
- Install a firewall program, especially if your computer is connected to the Internet 24 hours a day.
- Use a secure browser – software that encrypts or scrambles information you send over the Internet – to protect the security of your online transactions.
- Protect any financial information that you store on your computer with a difficult password.
- Before you dispose of your computer, use a wipe utility program to overwrite the entire hard drive, which makes the files more difficult to recover.
- Review a Web site's privacy policy before transacting any business through it. The Web site should contain a link to its privacy policy. Usually the link is located at the bottom of the page and is titled "Privacy Policy." A reliable privacy policy should explain what information the Web site collects from you, how it protects that information, whether it uses cookies, and whether it allows you to opt in or opt out of the Web site's data collecting, sharing, or retaining policies.

Control access to you and your credit history:

- Remove your name from mailing lists for approved lines of credit by participating in the credit bureaus' opt-out program; call 888.5.OPT.OUT (888.567.8688) to enroll. You will need to provide your social security number to verify that you are making the request, but this is a legitimate use of such information.
- Write to your bank, insurance company, and other financial institutions you do business with and tell them not to share your customer information with unaffiliated third parties. Under federal law, they are required to honor this request.
- Remove your name from national direct mail advertising lists by sending your name and address with a written request to DMA Mail Preference Service, Department 12059580, Direct Marketing Association, P.O. Box 282, Carmel, NY 10512.
- Participate in the national no-call registry by going online at www.donotcall.gov or by calling 888.382.1222 (TTY: 866.290.4236).
- If you are a member of the military and away from your usual duty station, instruct the three credit reporting agencies to place an active duty alert on your creditreports to help minimize the risk of identity crime while you are deployed. Visit https://www.annualcreditreport.com to request the alert.

Watch for signs of fraud:

- Review your bank and credit card statements monthly and alert creditors to any charges you do not recognize.
- Order a copy of your credit report at least annually and check it carefully (https://www.annualcreditreport.com).
- Review the earnings and benefits summary you receive from the Social Security Administration each year.
- Notify your creditors any time a bill is late to arrive, and verify that they have your correct mailing address.

**Protecting the Real You and Only You.**
The International Association of Chiefs of Police
515 N. Washington Street, Alexandria, VA 22314
Telephone: 1.800.843.4227
www.theiacp.org