



# State of New York Office of the Attorney General



## Tips For Protecting Your PRIVACY

## Don't Become A Victim of IDENTITY THEFT

ANDREW M. CUOMO  
Attorney General

# TABLE OF CONTENTS

|   |    |
|---|----|
| <i>Introduction</i> .....   | 1  |
| <i>Target Marketing</i> .....   | 3  |
| <i>Credit Bureaus</i> .....   | 3  |
| <i>Marketers and Mailing Lists</i> .....  | 6  |
| <i>Department of Motor Vehicles</i> .....                                       | 9  |
| <i>Phone and Address Directories</i> .....                                      | 10 |
| <i>Telemarketing</i> .....  | 11 |
| <i>Medical Records</i> .....  | 16 |
| <i>Internet Privacy</i> .....   | 20 |
| <i>Children's On-line Privacy</i> .....   | 25 |
| <i>Additional Privacy Laws Affecting Commercial Transactions</i> .              | 25 |
| <i>Unsolicited Faxes</i> .....  | 25 |
| <i>Electronic Funds Transfer</i> .....  | 26 |
| <i>Cable Communications</i> .....   | 26 |
| <i>Video Viewing</i> .....  | 26 |
| <i>Using a Credit Card or Writing a Check</i> .....                             | 27 |
| <i>Other Privacy Laws - Laws Affecting Public Agencies</i> .....                | 28 |
| <i>Social Security Number</i> .....   | 28 |
| <i>Personal Information Compiled by Federal<br/>    Or State Agencies</i> ..... | 29 |

|  |    |
|--|----|
| <i>Right to Financial Privacy</i> .....                            | 29 |
| <i>Drug Addiction and Alcoholism Treatment Privacy</i> .....       | 30 |
| <i>Family Educational Rights &amp; Privacy Act</i> .....           | 30 |
| <i>Library Records</i> .....                                       | 32 |
| <br>   |    |
| <i>Privacy &amp; Identity Theft: How to Protect Yourself</i> ..... | 32 |
| <br>   |    |
| <i>Tips on Avoiding ID Theft</i> .....                             | 33 |
| <i>Dealing with I.D. Theft</i> .....                               | 38 |
| <i>Law Enforcement</i> .....                                       | 38 |
| <i>Creditors</i> .....   | 39 |
| <i>Credit Bureaus</i> .....  | 40 |
| <i>Credit Freezes</i> .....  | 41 |
| <i>Banks</i> .....   | 45 |
| <i>Stolen Checks</i> .....   | 45 |
| <i>Social Security Numbers</i> .....                               | 48 |
| <i>Health Insurance</i> .....                                      | 48 |
| <i>U.S. Postal Service</i> .....                                   | 48 |
| <i>Investments</i> .....   | 49 |
| <i>Taxes</i> .....   | 49 |
| <i>Phone Service</i> .....   | 49 |
| <i>Motor Vehicles</i> .....  | 50 |
| <br>   |    |
| <i>Identity Theft Statutes</i> .....                               | 50 |
| <br>   |    |
| <i>Federal Law</i> .....   | 50 |
| <i>New York State Law</i> .....                                    | 51 |
| <br>   |    |
| <i>In Conclusion</i> .....   | 52 |
| <br>   |    |
| <i>Offices of the Attorney General</i> .....                       | 53 |

## *INTRODUCTION*

In the course of a day, you may write a check, charge an article of clothing, order a book on the Internet, apply for a new credit card, answer a product warranty form, withdraw money from an ATM, or purchase food and health and beauty aids with a store discount card. This electronic processing of personal data helps provide for personalization of services and special promotions and discounts. While you probably don't give these routine, convenient transactions much thought, others do!

Your personal information is a valuable commodity that, in the wrong hands, can be misused. Applying various schemes, a scam artist can capture your Social Security, credit card, or ATM number, birth date, and other identifying information, that you voluntarily provide to companies, to assume your identity. The thief then builds upon this initial information by posing as you and using trickery to collect more details, or by investigating you over the Internet. Once armed with this valuable information, the imposter applies for instant credit, opens bank or utility accounts, steals money from your existing accounts, and makes purchases in your name.

Identity theft, which is fast becoming the most prevalent financial crime in the country affecting nearly half a million new victims each year, goes to the very heart of "information privacy." Today, your personally identifiable data gleaned from independent transactions may be captured in computer databases and used for a variety of unrelated purposes by third parties, often without your consent. From morning until night, the details of your life are

being recorded, analyzed and sold at ever-decreasing cost and ever-increasing speed. The easy access to sensitive data may contribute to fraud and other criminal activities as well as to unsolicited mail, Internet and telephone offers.

Thus, in poll after poll, public concern for “information privacy” is mounting. *Information privacy is defined as your right to determine when, how and to what extent information about yourself is communicated to others and your ability to prevent the disclosure and dissemination of your personal, sensitive information beyond the legitimate purpose for which it was originally collected or disclosed.*

This brochure presents some information handling practices which will make it less likely that an imposter will steal your personal data. The menu of precautions – many easy, some more difficult, most inexpensive, few costly – will help reaffirm your control over your personal information. Though suggestions are offered, the choice of which strategies to use and how much information to disclose in your daily activities is yours! This guide provides an overview of the variety of federal and state laws which offer specific privacy rights. Many of these privacy statutes embrace specific core principles of fair information practices which govern the collection, storage and dissemination of data: notice; access; control; accuracy; security; and accountability and, finally, if you should unfortunately become a victim of identity theft, this booklet recommends measures to help in your recovery.

## ***TARGET MARKETING***

Exercising control over your personal information will enhance your privacy and reduce the likelihood of becoming an identity theft victim. Common sense dictates that the less information available about you, the less likely others will get their hands on it! You are your best advocate and protector!



## **CREDIT BUREAUS**

Currently, many marketers, especially credit card issuers, get your name and personally identifiable information from credit reporting agencies, often referred to as credit bureaus. If you've ever received an unsolicited "pre-approved credit card" offer, your name and address were probably supplied to this company by a credit bureau.

**The Federal Fair Credit Reporting Act (FCRA)** gives you the right to "opt-out" of having your name and address included in credit bureau marketing lists. In other words, you may contact credit bureaus to inform them that you don't want to be included on any list they supply to the marketers. This will reduce the volume of pre-screened credit and insurance offers you receive in the mail and limit the number of organizations that have information about you. By opting out of unsolicited credit offers, you also will eliminate a potential target of identity thieves, who use these solicitations to obtain credit cards in your name.

You can contact the credit bureaus to find out more about their opt-out procedures by calling **888-5OPTOUT (888-567-8688)**. Federal law requires credit bureaus to remove your listing for several years. Thus, being diligent about keeping your name on the lists will be necessary.

You should also **review your monthly credit card statements and your credit report at least once a year**, checking them for inaccuracies and fraudulent credit activity. Look for any debts you don't recognize and credit inquiries that you did not initiate. These entries might mean that someone is using your name to secure credit and purchase items, resulting in major financial headaches!

When you have been turned down for credit, and request your report within 60 days of this adverse action, or have been a victim of fraud, a copy of your report is free. Otherwise, there will be a nominal fee (approximately \$10.00) to obtain your report.

The three major credit bureaus may be contacted as follows:

**Trans Union**

P.O. Box 1000

Chester, PA 19022

(800) 888-4213 [www.transunion.com](http://www.transunion.com)

## **Experian National Consumer Assistance Center**

P.O. Box 9554

Allen, TX 75103-2104

(888) 397-3742 [www.experian.com](http://www.experian.com)

## **Equifax Information Center**

P.O. Box 740241

Atlanta, GA 30374-0241

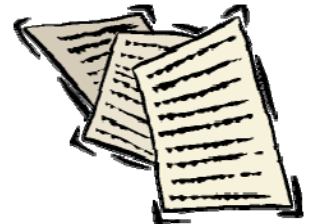
(800) 685-1111 [www.equifax.com](http://www.equifax.com)

The **Fair and Accurate Credit Transactions Act**, enacted in 2003, essentially expands on the consumer protections provided by the FCRA. Specifically, the FACT Act provides for the following:

- ▶ **One Free Credit Report Per Year** -- Each nationwide credit reporting agency must provide a report within 15 days of a consumer request by phone, Internet, or mail through a one-call centralized source to be established by the FTC. Specialty bureaus, such as landlord-tenant or insurance reporting services, will also provide reports.
- ▶ **Stronger Opt-out Notices for Pre-screened Offers of Credit** -- Notice must contain a phone number to opt out in an easy to understand format. The new law also extends the duration of the opt out by telephone from 2 years to 5 years.

- ▶ **Marketing Solicitation Restrictions** -- Consumers may opt out of receiving solicitations for marketing purposes based on information shared among corporate affiliates for at least 5 years, after which the consumer must be given notice and the opportunity to opt out again.
- ▶ **Protection of Medical Information** -- Credit agencies are prohibited from furnishing a report that contains medical information for insurance, employment or credit transaction purposes unless the consumer consents. Alternatively, the information may be reported if coded so as not to identify the provider or the nature of services or products. Creditors cannot obtain or use medical information in credit decisions. Medical information cannot be shared among affiliates.

## **MARKETERS AND MAILING LISTS**



When you provide your name and address to purchase merchandise, receive a service, or tend to your daily pursuits, this information may be “harvested” for other purposes. Many marketers exchange, sell or rent your transactional data as part of a mailing list. Your lifestyle, demographic, income and other information may be added to produce a more comprehensive profile for sale to third parties. You can take action to reduce the amount of information about you that is exchanged.

**Financial Institutions:** Contact your financial institution to opt-out of having your name, phone number, address and other financial information, including details about your account or payment history, disclosed to marketers. The **Financial Services Modernization Act of 1999**, requires financial institutions, such as your bank, thrift, credit card company or credit union, to provide a written notice of their data practices and a convenient way for you to exercise your right in restricting the release of personal information to marketing companies. This applies only to “non-affiliated” parties or companies that are not within the family of companies of the financial corporation, and therefore does not necessarily cover all disclosures. However, by contacting your financial institutions and opting-out, you limit who has knowledge of your account balance, your cash advances, and your purchases per year. You also take your name and phone number off many lists provided to telemarketers.

**Insurance Companies:** Most personal information handled by insurance companies is covered by the Financial Services Modernization Act. Insurers are required to send you a privacy notice and honor your preference to stop the disclosure of your data to unrelated businesses. Contact your insurance company for details about opting out of their marketing lists.

**Marketing Lists:** The Direct Marketing Association, a trade organization that represents over 4,500 marketers nationwide, offers Mail Preference Services, which allow you to opt-out of direct mail and marketing lists from member companies. To have your name removed from their mailing lists, write to:

## **Direct Marketing Association**

Mail Preference Service

P.O. Box 282

Carmel, NY 10512

<https://www.the-dma.org/consumers/index.html>

Privacy is a core issue that, together with customer relations, dictates how a business treats its consumers. A growing number of companies keep lists of their customers who do not want their personal information--including buying habits--to be disclosed to other businesses. You can contact companies with which you do business and inquire about their privacy policies. Although many companies are not required by law to remove customer names from their mailing lists, raising this issue may cause these businesses to change their data practices.

**Supermarket and Membership Discount Cards:** Numerous supermarkets, pharmacies and other businesses issue discount cards for their customers to receive special sale prices and coupons in the mail. Some of these retailers ask you for sensitive information to join their program and track your purchases. Manufacturers and others are interested in purchasing this data.

If you are concerned about revealing this data, you should think twice about using these discount cards. Do not buy anything with a discount card that you don't want publicly known and marketed. If you use your supermarket card to pay your bill by check, inquire into alternative methods.

**Warranty Cards:** Many manufacturers provide warranty cards requesting personal information including household income. Most of these cards leave you with the impression that they must be completed and returned to the company in order to get the warranty protections. This is not the case if you have a full warranty. As long as you can verify a purchase (usually with a receipt), the warranty is in effect. Filling out and returning these forms to the manufacturer will continue the profiling process and only place your name on more mailing lists.

In the case of a limited warranty, however, the warrantor can condition its performance on the return of the card, *provided* this fact is disclosed. It might be useful to write to your warrantor to request that any personally identifiable information provided not be shared with marketers.

**Surveys:** Surveys usually do not disclose how your self-reported data is used. Often the information is processed and sold. When completing questionnaires, you should be sure of the survey's purpose and inquire as to who will have access to your information.

**Motor Vehicles:** In 1999, Congress amended the **Federal Drivers' Privacy Protection Act** to provide an important privacy right to all license holders across the country. The Act requires state motor vehicles departments, including the New York State Department of Motor Vehicles, to secure your consent *prior* to having your personally identifiable information— name, address,



Social Security number, telephone number, driver identification number and photo – included in lists bought and supplied to most marketing entities. Information on your vehicular accidents, driving violations and driver status is not afforded these privacy protections.

Of course, this law doesn't preclude the State from providing information about you to those who have an authorized and legitimate purpose, like law enforcement, vehicle safety or insurance underwriting. For example, DMV still will provide your insurance carrier access to your information because it has a legitimate need to verify your driving record and history.

**Phone & Address Directories:** Obtaining an unlisted, non-listed or non-published telephone number, or simply listing your phone number with-out the street address in the telephone directory, will help keep your name and personal information off marketing lists and reduce unsolicited offers. While an unlisted or non-listed telephone number can be obtained from a directory assistance operator, a non-published number cannot. For more information, contact your local phone company. Of course, not listing your number may make it more difficult for others to reach you including your friends and colleagues.

Also, you can write to the following companies that compile street address directories to request your name and address be removed:

**Haines & Co.**  
Criss-Cross Directory

Attn: Director of Data Processing  
8050 Freedom Avenue, Northwest  
North Canton, OH 44720  
(800) 254-3449

**R.L. Polk & Co.**

Attn: List Suppression Files  
26955 Northwestern Highway  
South Field, MI 48034  
(800) GO 4 POLK or (800) 464-7655



***TELEMARKETING***

New Yorkers frequently ask the Attorney General's Office how to stop intrusive telemarketing calls. With all the trafficking in marketing lists, it is difficult to completely shield oneself from these calls. However, certain laws and practices give you the ability to greatly restrict them.

You may restrict the number of telemarketing calls on a national basis by registering for the new **national list at:**

**WWW.DONOTCALL.GOV** or call **(1-888-382-1222)** (TTY **1-866-290-4236**), from the number you wish to register. You can list your home and/or mobile phone for free. Telemarketers have up to three months to stop calling you. Your information will be maintained on the registry for a period of five years.

The millions of telephone numbers listed on New York State's **Do Not Call Registry** have been merged with the National Do Not Call Registry. While the Consumer Protection Board of New York State will continue to enforce telemarketer compliance with the state "Do Not Call" law and regulations, the Federal Trade Commission (FTC) will maintain New York's "Do Not Call" Registry as part of the National "Do Not Call" program. Violators of the Federal Rule will be subject to a fine of up to \$11,000 per violation. Under the New York State law, violators can be fined up to \$5,000 per violation.

Registration reduces the number of unsolicited calls placed to your home, but it will not end all telemarketing solicitations. You may still receive calls from: charitable and religious organizations; political parties; companies with which you have a prior business relationship; and marketers who wish to arrange for a face-to-face presentation before accepting payment.

If your number has been on the National Do Not Call Registry for at least three months and you receive a call from a telemarketer that you believe is governed by the National Do Not Call Registry, you can file a complaint with the FTC at:

<https://www.donotcall.gov> To file a complaint, you must know either the name or telephone number of the company that called you, and the date of the call.

If you wish to have more flexibility and restrict calls on a company by company basis, you have this right under the federal **Telephone Consumer Protection Act of 1991** (TCPA). Companies soliciting through telemarketing are required to keep their own "do not call"

list and honor your request not to receive future solicitations for ten years. **Remember: Each time you receive a call from a different marketer you must request that the entity not call you again.**

Under the federal **Telemarketing Sales Rule**, charities and for-profit telemarketers calling on their behalf, must honor your request not to be called again and place your name on their own “do not call” list.

Should you receive a call that you think is in violation of the federal or state law, write down the following to enforce your rights: **date and time of call; name of the company; name and address of telemarketer; and the product or service.**

If you believe you’ve been called by a company in violation of the TCPA, contact the Attorney General’s Office at: (800) 771-7755.

**Restricted Hours:** The TCPA also prohibits telemarketers from placing calls to your home between the hours of 8 P.M. and 9 A.M. local time unless they have received your prior express consent or if you have an established business relationship.

**Identification of Seller:** Federal and state law requires telemarketers to identify the business on whose behalf the solicitation is made and the purpose of the call immediately after contacting you.

**Automatic Dialing Devices and Pre-Recorded Messages:** The use of “autodialers” and pre-recorded messages in telemarketing also is regulated by federal and state law. An autodialer is equipment that stores and dials telephone numbers in sequential order or at random. Autodialed or prerecorded telemarketing calls cannot be placed to your home except for the following:

- ▶ emergency purposes;
- ▶ when you have given prior consent;
- ▶ non-commercial calls (charities and not-for-profit organizations, polling organizations, political or governmental agencies);
- ▶ calls from companies with which you have an existing business relationship.

Autodialed or prerecorded messages to emergency numbers, hospitals, cellular telephones, pagers, or any service for which you are charged are prohibited. However, they are allowed in emergencies or if you gave your prior express consent.

Any pre-recorded telemarketing message must state at the beginning: the nature of the call and the name of the person or on whose behalf the message is being transmitted. At the end of the call, the message must provide the address and telephone number of the person on whose behalf the telemarketing call is being made.

Pre-recorded telemarketing messages using an autodialer must disconnect your telephone line within five seconds of the telephone

network's signal to the caller indicating that you have hung up. Picking up the telephone receiver before this signal reaches the telemarketer may cause some recorded messages to continue playing.

**Custom Calling Services:** Your local phone company may offer services which can be used to restrict unsolicited calls.

- ▶ **Caller ID** displays the number of the person calling. State law prohibits telemarketers from using devices to block identification information from appearing on your Caller ID box. Under a federal rule, telemarketers must also transmit Caller ID information to help consumers choose which sales calls they want to take.
- ▶ **Per-Call Blocking:** This technology will prevent or block your phone number from appearing on a Caller ID box only when you enter code “\*67” before dialing.
- ▶ **Per-Line Blocking:** If you select this option, your phone number will automatically be blocked for most calls. Thus, if you call someone who subscribes to Caller ID, the display will read “private,” or some other word instead of your phone number.

Contact your local phone company for more details about these blocking options and other ways to shield your number.

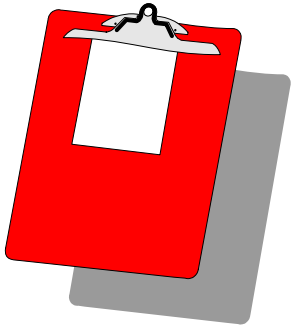
**Answering Machine:** To avoid solicitations, you may want to

screen your calls with an answering machine. Most marketers will hang up once they hear a recorded message!

**Restricting Access:** Be careful with your phone number. Release your telephone number only to those that need to have it. Avoid printing your phone number on your checks and on surveys and sweepstakes-contest forms.

## ***MEDICAL RECORDS***

You reveal sensitive, personal information to your health care provider. This information is then often shared with others including insurance companies, data clearinghouses, pharmacies, researchers, government agencies and employers, for a variety of purposes. As more of your medical information is collected and maintained in computerized databases, it will be easier for people to gain access to your records and use the data for activities unrelated to health care.



**Free Health Screenings:** Remember that blood pressure screening you participated in at the mall or the cholesterol test you had done at the county fair? These may be convenient ways to learn important things about your health. Ask whether information from those events is collected and sold to data banks and businesses for various commercial purposes. Marketers also may be sold medical information about you when you complete an informal health-related survey. Some data brokers sell lists of patients and their illnesses to third parties and employers. Be cautious when

providing medical information for surveys and participating in health screenings, and ask how the information will be used and who will have access to it. You should read any posted privacy policy and be aware of your choices.

**The Medical Information Bureau (MIB)** is a membership association of more than 600 insurance companies. When applying for insurance, you may be authorizing the company to check your information with the database maintained by MIB. While not everyone has a file, you may want to find out if your medical history is in MIB's database, and verify that it is correct. You have the right to see and correct your record by contacting:

**Medical Information Bureau**

P.O. Box 105, Essex Station

Boston, MA 02112

(617) 426-3660

[www.mib.com](http://www.mib.com)

A nominal fee (approximately \$8.50) is generally charged for a report. However, it is free if you received a letter from an insurance company indicating that they used MIB information to make a decision about you.

**Internet Medical Sites:** A significant amount of health-related information is found on the Internet. Several sites ask you for detailed information as a condition to accessing the material. Some websites may not tell you what they do with your information and to whom they release the data. You may also unintentionally reveal

sensitive information simply by visiting a site. While chat rooms or on-line discussion groups are used to share information about specific diseases and conditions, there is no guarantee that the details you disclose in any of these forums are kept confidential. These sites are increasingly used by drug manufacturers and others to promote products. You should avoid registering your name on websites and use a pseudonym and a non-name specific electronic mail address.

The federal **Health Insurance Portability and Accountability Act** regulations establish minimum privacy standards affecting the use, maintenance, and disclosure of personally identifiable health information by health care providers, health insurance plans, employers, researchers, and government agencies. Basically, you will have more knowledge about, and potential control over, what information is shared, with whom, and for what purposes. Generally, treatment providers and health plans must notify patients about their privacy rights and how their information can be used. For some purposes (treatment, payment and health care operations), the regulations permit a provider to use and disclose health information without the individual's permission, authorization or consent and with only a few restrictions. In lieu of obtaining an individual's permission, treatment providers must make a good faith effort to obtain the individual's written acknowledgment of receipt of the entity's notice of privacy practices. In other situations, the regulations, require the treatment provider or health plan to give the individual the opportunity to object to the disclosure. An individual has the right to request that the treatment provider or health plan restrict uses or disclosures of

health information about the individual to carry out treatment, payment or health care operations. However, the entity is not required to agree to such restrictions. Further, the regulations require entities to obtain an individual's prior written authorization to use or disclose health information for "marketing" of non health-related products. Additionally, an entity does not need patient authorization if it uses or discloses health information for marketing that occurs face-to-face or if the marketing involves a promotional gift of nominal value. At the same time, entities that receive your health information will be responsible for ensuring that the information is secured effectively. With limited exceptions, you will have a federal right to inspect and obtain a copy of your health record and learn who gained access to it. You also will have the right to amend or supplement your record. For more details, contact the U.S. Department of Health and Human Services (HHS) toll-free at (877) 696-6775 or visit its website at [www.hhs.gov](http://www.hhs.gov). HHS's Office for Civil Rights enforces these privacy regulations.

**The New York State Managed Care Bill of Rights** Law requires health maintenance organizations to provide, upon your request, information about its procedures in protecting enrollee medical and other information. It would be advisable to check this information with your plan.

**Access to Medical Records:** New York State law gives you the right to access your medical records from providers or health care facilities. No more than 75 cents a page for paper copies of your treatment information and test results may be charged. However,

providers may charge the actual reproduction costs for x-rays. Whenever a health care provider discloses your medical information to a third party, a notation of the name of the party and the purpose for the disclosure must be entered in your file. You may challenge the accuracy of the data in your record and insert a brief written explanatory statement which will be released whenever the information at issue is disclosed.

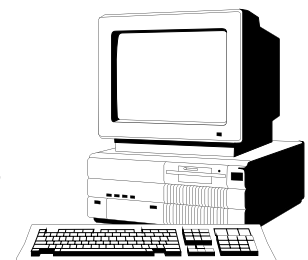
If you have questions about accessing your medical records or complaints about the exchange of your medical file between other entities, please contact the Attorney General's helpline at: (800) 771-7755.

**Authorization Forms:** It is important to read medical release forms carefully. Before signing any form, you should find out to whom you are authorizing the release of your records and for what purpose. You may be able to limit disclosure and restrict further release of the information by changing the wording in the document. Make sure to initial and date your revisions.

## ***INTERNET PRIVACY***

The information superhighway is paved with new opportunities and benefits. However, unless you are aware of the privacy rules of the "virtual road," you may encounter potholes as you travel in cyberspace.

The computer's ability to compile and sort vast amounts of information and the Internet's ability to



distribute it globally magnify your opportunities and privacy concerns. With more computerized information about you, you are exposed to greater risk that someone may misuse your data.

**Privacy Policies:** Many websites require you to register or ask that you complete surveys eliciting private details. Some sites keep profiles on their visitors, and even purchase information about you from other marketers. Your profile can be sold too. An on-line business may monitor your activities so that it can target information and advertisements matched to your interests.

Look for privacy policies that explain the need for the information requested from you, the use of the data, and steps taken to safeguard it. Sites that are most sensitive to your privacy concerns will have policies displayed clearly and conspicuously and offer you a choice in restricting the release of your data. You can also look for a privacy “seal of approval” offered by various organizations, on the first page of a site. If a privacy policy is not posted, you may want to ask the company questions -- and if its answer is unsatisfying, you should consider not returning to the site and taking your business elsewhere.

Be particularly wary before providing any information that can be used to steal your identity and facilitate fraud, such as your Social Security number and mother’s maiden name.

**Safeguard your password** as cyberspace has its share of scam artists and “snoopers.” Your password is the key to your account. Use a combination of letters, numbers and symbols for your

password. Employees of your service provider should **never** request your password. If they do, report it to your provider immediately.

**Shopping Online:** Always make sure that a website is secure before providing any financial data, such as credit card or a bank account number. Secured sites use encryption to scramble your information as it is transmitted over the Internet. You should look for website addresses preceded by **https** with a yellow or golden closed lock or an unbroken key at the bottom of your browser window. If you are ill at ease providing your billing information over the net, ask the company about alternate methods of ordering.

**Cookies:** Some websites use **cookies**— files placed on your hard drive so the site can “remember” information about you or your computer. While a cookie is not a spy device or a way for a website to secretly discover your personal information, it may allow a site to track information about your browsing habits or navigational information on an anonymous basis, after multiple visits to that website. If, for example, you linger over a product or a subject, it may be recorded. Subsequently, you might see ads on the site that have been customized for you. Some companies may eventually use cookies to help link currently anonymous navigational data to personally identifiable information provided by users upon registration with the site or purchase of merchandise.

Most browsers allow you to reject cookies or warn you before one is accepted by your computer for storage. To learn more about cookies on your computer and what you can do about them, consult your browser's help or tutorial feature. Programs also are available that allow you to automate the process of reviewing or rejecting cookies. For additional information on cookies, visit: <http://www.junkbusters.com/ht/en/cookies.html>

**E-Mail:** While E-mail is relatively private, don't type anything into an electronic message that you wouldn't want posted in public. If you receive e-mail which appears to be from your service provider or any other company asking for credit card information, DO NOT REPLY.

**Unsolicited E-mail / Spam<sup>®</sup> :** Unsolicited commercial e-mail may be a nuisance and can even pose certain dangers. Be aware that your e-mail address can be captured even if you don't explicitly provide it. Often, "spammers" – individuals and entities that send numerous unwanted e-mail advertisements and scams – use software to "harvest" e-mail addresses from chat rooms, webpages, on-line bulletin boards and news group postings.

Spammers tend to use on-line user profiles to help them select their targets. As a result, you should be careful revealing information about yourself including your e-mail address.

### **How do you avoid unsolicited e-mail?**

- ▶ **Do not respond or retaliate.** If the return address is real,

the spammer will realize that your account is active; if it's fake, your reply will cause problems for an innocent system administrator.

- ▶ **Alert your ISP.** Forward suspected spam to your Internet Service Provider (ISP) -- usually to the webmaster address.
- ▶ **Use filters.** Many ISPs block incoming bulk mail from known spammers and those using falsified return addresses. Some providers also offer tools to scan messages for repeated use of terms such as "get rich" or "XXX" and block them at your request.
- ▶ **Exercise Caution.** Delete e-mail from unknown sources. Don't download anything unless you know the sender as "harmless" e-mail enclosures may contain a virus or spyware.
- ▶ **Use a forwarding address.** Many companies, such as hotmail.com and bigfoot.com, offer free e-mail accounts which can be used to screen messages. Those messages you want are forwarded to an account whose address you keep private. Some of these accounts are equipped with filtering capabilities.
- ▶ **Have your name and e-mail address removed from some mailing lists by visiting [www.e-mps.org/en](http://www.e-mps.org/en).**

- ▶ **Do not submit your e-mail address or any other personal information to any site claiming to be a “National Do Not E-mail Registry” as this is a scam.**
- ▶ **Check with your service provider for additional ways to limit unsolicited e-mail.**

**Cyberspace Traveling with Children: The Federal Children’s On-line Privacy Protection and Parental Empowerment Act** requires commercial websites to obtain prior parental consent before collecting personal information from children under 13. As a parent, you have the right to be notified about data collection and use practices and to access and review personally identifiable data about your children. In addition, the collection of personal information for a child’s participation in an on-line game, contest, or other activity must be limited to what is reasonably necessary for the activity.

## **ADDITIONAL PRIVACY LAWS AFFECTING COMMERCIAL TRANSACTIONS**

### **UNSOLICITED FAXES**

Regulations issued by the Federal Communications Commission (FCC) prohibit the transmission of unsolicited advertisements to fax machines.

Businesses with which you have an existing relationship are exempt from this prohibition. However, if you inform the business that you no longer want such faxes, it must comply. FCC



regulations also require all faxes to be clearly marked on the first page or on each page with the following information: the date and time of the transmission; the identity of the sender; and the telephone or fax number of the sending machine. Senders are also required to provide notice on how recipients may opt-out of future faxes.

## **ELECTRONIC FUNDS TRANSFER**

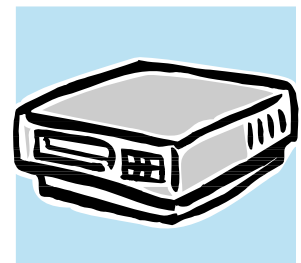
Federal law requires financial institutions to make certain disclosures at the time you contract for an electronic fund transfer service or before the first transfer is made involving your account. The financial institution must disclose the circumstances under which it may provide information about your account to third parties.

## **CABLE COMMUNICATIONS**

The **Federal Cable Communications Policy Act** requires cable television operators to notify you annually about data collection and disclosure practices and your right to inspect and correct errors. It also prohibits the companies from collecting or disclosing your personal data without your consent.

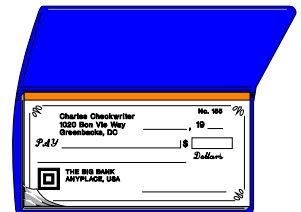
## **VIDEO VIEWING**

According to the **Federal and State Video Privacy Protection Act**, you have the right to restrict the disclosure of your name, address and information about



your video viewing habits for marketing purposes. Generally, video providers are prohibited from disclosing your viewing selections without your consent. They may release your name and address on mailing lists provided that the lists do not disclose your viewing preferences and you were given the opportunity to prohibit such disclosure. Written notice of these data practices must appear in your video agreement. However, the videotape provider can disclose your data: pursuant to a grand jury subpoena; a court order; a warrant; pursuant to a civil action commenced by the company; to enforce collection of fines for overdue or unreturned tapes; to any person who possesses your written consent; and in the ordinary course of doing business. Wrongful disclosure of personal information is subject to damages of no less than \$500, plus court costs and reasonable attorneys' fees.

## **USING A CREDIT CARD OR WRITING A CHECK**



In order to prevent fraud, state law prohibits a merchant from recording your personally identifiable information such as your address or telephone number on a credit card transaction form, unless it is necessary for the shipping, delivery or installation of merchandise or if your credit card company does not require authorization for the merchant to complete the sale. State law also restricts merchants from recording your credit card or Social Security number on a check, gift certificate, traveler's check or money order. The merchant, however, is allowed to ask you to display a credit card as proof of identification or credit-worthiness and write down the card type

and its expiration date.

## **OTHER PRIVACY LAWS** **AFFECTING PUBLIC AGENCIES**

### **SOCIAL SECURITY NUMBER**

**The Federal Social Security Privacy Act of 1974** requires all government agencies -- federal, state, and local -- seeking Social Security numbers (SSNs) to disclose their authority for this request, indicate whether it is mandatory or voluntary; explain how your number will be used; and tell you the consequences for failing to disclose it. This law states that you cannot be denied a government benefit or service if you refuse to provide your number unless the disclosure is required by law or the disclosure is to an agency which was using Social Security numbers prior to January, 1975, the effective date of the Privacy Act. For example, the NYS Department of Motor Vehicles indicates on its application for a driver's license its authority to collect your SSn and advises you that SSNs will not be released to the public.

Private companies are not required to follow the Privacy Act of 1974, and generally your recourse is to find another company with which to do business if you are concerned about its information-handling policies.

Usually, the government does not require you to provide your SSn to private businesses -- including health care providers and insurers

-- unless you are involved in a transaction in which the IRS needs that information (e.g. banking, stock market activity, employment earnings, and payroll tax reports). Because your SSn must be included on sensitive financial and other governmental documents, it is wise to be careful with it and limit other uses. Therefore, when a business requests your SSn, you may want to ask a supervisor about using an alternative number.

## **PERSONAL INFORMATION COMPILED BY FEDERAL OR STATE AGENCIES**

**The Privacy Protection Act:** Federal and state law protects your personal privacy by requiring government agencies to:

- ▶ maintain only personal information that is relevant and necessary;
- ▶ explain their authorization and purpose for collecting your personal data, the consequences for failing to provide it, and any disclosures of your records outside the agency;
- ▶ provide you with access to your records and an opportunity to correct or challenge that information; and
- ▶ keep an accounting of all disclosures of your file.

## **BANK RECORDS**

**Under the Right to Financial Privacy Act,** federal agencies seeking access to your private financial records must either (1) notify you of the purpose and give you an opportunity to challenge the disclosure in court; or (2) obtain a court order for direct access

to your information. The law also prohibits any federal agency that has obtained access to your financial records from disclosing the information to another agency without (1) notifying you; and (2) obtaining certification from the receiving agency that the records are relevant to a legitimate law enforcement inquiry. A grand jury subpoena is an exception to the Act.

## **DRUG ADDICTION AND ALCOHOLISM TREATMENT**

**Federal Drug and Alcoholism Confidentiality Laws:** These statutes generally prohibit the disclosure of information collected from federally-funded research and treatment of substance abuse for any other purpose, except in cases of medical emergency or where a court order has been issued. This information is especially protected from use against the subject in any criminal proceeding.

## **EDUCATION RECORDS**

**The Federal Family Educational Rights and Privacy Act** prohibits schools or educational agencies receiving public funds from releasing or using education records (or personally identifiable information) to any individual, agency, or organization without the written consent of the student or parent of a minor student. Medical and health records that the school creates or maintains are also covered. Exceptions include: (1) under subpoena; (2) other school officials, including teachers within the educational institution or agency, who have a legitimate purpose; (3) officials of other schools in which the student seeks or intends to enroll; (4) appropriate federal, state and local authorities; (5)

organizations conducting studies or developing predictive tests, provided that this does not permit the personal identification of students and those records will be destroyed when no longer needed; and (6) other appropriate persons in emergency situations, if such information is necessary to protect the health or safety of the student or other persons.

The same rules restricting disclosures apply to records maintained by third parties on behalf of schools, such as researchers, psychologists, or medical providers who work for or are under contract to the educational institution.

In addition to restricting disclosure, the law also allows the student or parent access to the relevant educational records. If upon review, an error is found, the student or parent may request changes or corrections. Should the request be denied, a hearing must be held. If the matter remains unresolved after the hearing, a written explanation of the student's or parent's objection may be inserted in the record. These provisions do not apply to grades and educational decisions about the student that school personnel make.

Information collected from students through publicly-funded surveys, research or evaluations also must be available for parents to review. Those conducting the surveys are required to obtain prior consent from the parent if they plan to collect information from students concerning:

- ▶ Political affiliation or income;

- ▶ Mental and psychological problems;
- ▶ Sexual behavior and attitudes;
- ▶ Illegal or self-incriminating behavior;
- ▶ Critical assessments of other family members; or
- ▶ Privileged information given to lawyers, physicians, or clergy.

**Social Security Numbers:** State law prohibits schools from using Social Security numbers to identify students either on ID cards, class rosters, grade lists or in student directories.

**Library Records:** According to state law, school or public library records containing your personally identifiable information may only be disclosed for the proper operation of the institution; upon your request or consent; or pursuant to a subpoena or court order.

### ***IDENTITY THEFT: Protect Yourself***

Identity theft is quickly becoming the most prevalent and costly financial crime in the nation. Although estimates vary, between 500,000 to 750,000 people each year have their identities stolen, costing them and the financial industry billions of dollars. Credit Bureaus actually report receiving as many as 1,200 inquiries *per day* about fraud.

Identity theft occurs when someone invades your life taking pieces of your personally identifiable information as his or her own, to apply for credit cards and loans, open bank and utility accounts

and make purchasers at your expense! Often, you are unaware that your identity has been stolen until your credit card, loan application or check is refused or bill collectors demand payment of unauthorized charges.

This criminal activity has the potential of emptying your bank accounts, maxing out your credit cards, or holding you responsible for loan payments and liability on purchases you never made.

Identity theft can ruin your credit history and reputation!

The nature of identity theft has changed dramatically over the past few years. No longer does a thief need to steal your wallet or credit card to gain access to your accounts. Today's identity thieves are information seekers who find bits of information about you by sorting through trash for discarded receipts and statements, spying for your PIN number at an ATM machine or telephone booth, accessing public records, posing as yourself to secure information or misrepresenting themselves to obtain your private data, hacking into computer websites, swiping your credit card in a device that steals the encoded information, and even stealing from your mailbox.

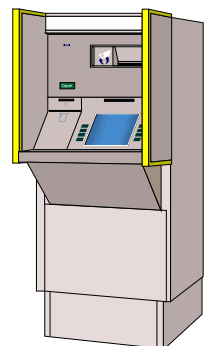
## **TIPS ON AVOIDING I.D. THEFT**

- ✓ **Be careful about disclosing your personally identifiable information**, such as your mother's maiden name and Social Security number. Inquire about how your data will be used and who will have access to it. You should ask if you can restrict disclosure.





- ✓ **Never provide any personal, bank account, or credit card information** to anyone who contacts you through a telephone or Internet solicitation. Any reputable company will mail information about itself and the products or services it's selling.
- ✓ **Do not leave behind any credit card receipts, including carbons. Check your credit card monthly statements** to guard against incorrect or fraudulent charges. If your statement does not arrive on a timely basis, contact your creditor immediately.
- ✓ To minimize your exposure if your wallet is lost or stolen, **limit the number of credit cards and other items with personally identifiable information** that you carry. Do not carry your credit cards in your checkbook.
- ✓ **Sign your credit cards as soon as you receive them.** Also, **cancel all inactive accounts.** Even though you do not use them, those accounts appear on your credit report, which can be used by thieves. If a new card does not arrive when you expect, you may need to cancel it and order a new card and number.
- ✓ **Provide written notification to your credit card companies in advance of an address change.**



- ✓ **Memorize your ATM number and keep it secret.** Many ATM frauds occur because cardholders wrote their access numbers on their cards or on slips of paper conveniently accessible.
- ✓ **Tear up all ATM and bank receipts,** old insurance forms, bank checks, expired charge/credit cards, and any other papers that include your personal information and account numbers. This includes pre-approved credit card solicitations! Thieves often search through your garbage to find these forms and use them to apply for credit in your name.
- ✓ **Keep items with personal information in a safe place.** Maintain a list of all credit cards, account numbers, expiration dates, and the customer service phone numbers in a secure place so that you can quickly call your creditors in case your cards are lost or stolen.
- ✓ **When creating passwords or PINs,** do not use the last four digits of your Social Security number, your birth date, middle name, mother's maiden name, address or anything else that could be discovered easily by thieves.
- ✓ **Do not leave envelopes containing your checks or other sensitive information in your home mailbox.** Due to the increased risk of theft, it is best to mail bills and other letters at the post office, rather than leaving them in your mailbox for the postal carrier.



- ✓ **When ordering new checks**, instead of having them mailed to your home (where they could be stolen from your mailbox), have them shipped to your bank for pick up.
- ✓ **Do not display personal or family information on the Internet or on a home page.**
- ✓ **Beware of phony ID Theft prevention services which are schemes to secure personal information.**
- ✓ **Consider placing a security freeze on your credit file to block someone from opening a new credit account using your name or personal information by contacting the three credit reporting agencies by mail.**

## **DEALING WITH I.D. THEFT**

If you suspect that someone has been using your name or personally identifiable information to make purchases or get credit, you need to take action immediately to minimize the damage. Because each case is different, you may only have to follow the steps that are applicable to your situation.



**Law Enforcement:** Report any fraudulent activity to the appropriate police or sheriff's department with jurisdiction in your area. Give them as much documented evidence as possible. The federal **Identity Theft and Assumption Deterrence Act** criminalizes fraud in connection with the theft and misuse of

personal data. Be sure to keep a copy of the police report generated as credit card companies and others often require it to verify that there was a purported crime before investigating.

The **Federal Trade Commission (FTC)** offers assistance to identity theft victims. Contact them at (877) IDTHEFT or you can visit its website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

**Creditors:** Report the problem to the creditor associated with the fraudulent activity both by telephone and then with a detailed follow-up letter. Keep copies of all correspondence.

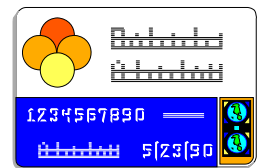
**Lost or Stolen Credit Cards:** Contact your credit card issuer or bank, as applicable. Under federal law, your liability for unauthorized charges to your account is limited to \$50; however, if you report the loss of your card prior to it being fraudulently used, you can't be held responsible for any unauthorized charges.

**Fraudulent Charges Appear on your Statements:** If you believe there are fraudulent or erroneous charges on your existing credit account, contact the issuer. The Federal Fair Credit Billing Error rules require credit card companies to remove disputed items from your bill when investigating. Under these rules, creditors must have procedures for resolving billing mistakes. A phone call is only sufficient to inquire into procedures for disputing the item. All disputes must be in writing. The letter must reach the creditor within 60 days of the mailing of the bill in order for your rights to be protected! The creditor is required to respond to your complaint in writing within 30 days and resolve the matter within two billing cycles (not more than 90 days).

More information about credit billing errors is available through the Attorney General's office by calling the consumer tip line at: (800) 771-7755.

The federal **Fair Debt Collection Practices Act** will protect you from a debt collector's unfair or deceptive practices. You can stop a collector from continuing to contact you by writing a letter documenting the fact that you were a victim of identity theft. Include a copy of the police report.

**Password Accounts:** If you have closed a credit card account due to fraud and opened a new one, insist on a password-only account.



**Credit Bureaus:** Immediately call the fraud helplines of each of the three major credit bureaus to inform them of the theft or fraud. Request that your account be **flagged** for fraudulent activity including a statement that creditors should call you for permission before they open any new accounts in your name. Future creditors will then be alerted to past problems and take extra precautions before granting credit. You may be required to file an ID Theft FTC Affidavit.

**Trans Union Fraud Victim Assistance Department**  
P.O. Box 6790  
Fullerton, CA 92634  
(888) 909-8872

## **Experian Consumer Fraud Assistance**

P.O. Box 9554  
Allen, TX 75013  
(888) 397-3742

## **Equifax Consumer Fraud Division**

P.O. Box 740256  
Atlanta, GA 30374  
(888) 766-0008

You should inquire into their procedures for getting a statement attached to any fraudulent information in your credit file so that potential creditors have access to the most recent information.

**Credit Report Security Freezes:** New York State law enables consumers to place a security freeze on their credit file to prevent someone from opening credit cards or other lines of credit in another person's name. The freeze takes effect within five business days after the consumer's letter is received by each of the three credit reporting agencies. The first request to place a security freeze on the credit file is free. However, a \$5 fee can be charged for subsequent requests, as well as to remove or temporarily lift the freeze. No fees are charged to victims of identity theft who provide a police report or an ID Theft FTC Affidavit.

Under federal law, victims of fraud are entitled to receive **a free copy of their credit reports**. It is advisable that you exercise this

right as soon as possible.

The **Fair and Accurate Credit Transactions Act**, provides consumer protections to assist victims of fraud. Some of the key provisions include:

- ▶ **One Call Fraud Alerts** -- Consumers who believe that they are or might be a victim of fraud can add an alert to their files with a nationwide consumer reporting agency which will be maintained for at least 90 days. The agency must refer the alert to other credit agencies and provide the information each time a credit score is generated. The agency is also required to notify the consumer of the right to a free credit report within three days of a request.
  
- ▶ **Extended Alerts** -- This alert may be included in the credit file for seven years where a consumer provides a law enforcement agency report to the credit agency. The agency must exclude the consumer from any pre-screening list or list generated to sell to users for transactions not initiated by the consumer for five years. The agency is also required to notify the consumer of the right to two free credit reports within 12 months of the alert.
  
- ▶ **Duty to Honor Fraud Alerts** -- Users of reports and scores cannot issue a new credit line, extension of credit, new cards or a higher credit limit on existing accounts unless the request is verified by the consumer.

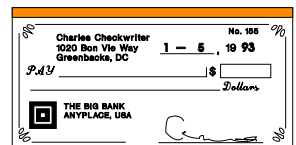
- ▶ **Block Trade Lines** -- Credit reporting agencies are required to block fraudulent trade lines when a consumer provides an ID theft report that has been filed with a law enforcement agency. Agencies must also notify furnishers of the block. If the block is rescinded, the agency must notify the consumer of that action and reason within five business days.
- ▶ **Prevent Repollution** -- Creditors and others who provide information to credit reporting agencies and who are notified of an ID theft trade line block must maintain procedures to prevent refurnishing (or repollution) of the information resulting from the ID theft without subsequent verification.
- ▶ **Prohibit Selling or Placing for Collection Identity Theft Debt** -- No person or business may sell, transfer, or place for collection any entry or debt subject to an ID theft trade line block once the creditor has notice of the block.
- ▶ **Notification Duties on Debt Collectors** -- Any third party debt collector who is informed that the debt may be fraudulent must notify the third party and provide the consumer with information on debt collection rights.
- ▶ **Access to Business Records** -- Any ID theft victim with a police report may request and secure copies of records from businesses where accounts were opened or goods or services purchased in their names. Businesses may take up to 30 days to respond.

- ▶ **Access to Credit Scores** -- Upon request by a consumer, credit bureaus must provide credit scores, and information on up to 5 key factors adversely affecting a consumer's credit score. A reasonable fee may be charged.
- ▶ **Mortgage Lenders** are required to provide credit scores, and information on key factors that may lower a consumer's score to loan applicants at no cost.
- ▶ **Notification of Negative Information to Customers** -- A financial institution submitting negative information to a national credit reporting agency must give consumers one-time written notification of their actions.
- ▶ **Time Restriction on Reinvestigations** -- Establishes a 45 day limit on investigations by credit reporting agencies of disputed items resulting from free report requests.
- ▶ **Dispute Information with Reporters** -- Consumers have the right to dispute incorrect information directly with the furnisher of the information.
- ▶ **New Standards for Furnishers** -- Furnishers are required to update their records by changing records, deleting records, or permanently blocking information to credit agencies of information found to be inaccurate or incomplete. A furnisher may not report information that it “knows or has reasonable cause to believe” is inaccurate.

- ▶ **Address Verification** -- Requires credit reporting agencies to notify anyone requesting a consumer's report if there is a discrepancy between the address on the request and the address in consumer's file. The credit card issuer will be required to conduct special verification procedures when notified of change of address from a cardholder and receives a request for additional or replacement cards.
- ▶ **Truncation of Numbers** -- A consumer may request that his/her credit report truncate their Social Security number. Credit card machines must cease printing credit and debit card numbers on receipts by 2007.

**Banks:** Contact your financial institution to report **lost or stolen ATM/Debit Cards**. Federal law provides that your liability for unauthorized charges is limited to \$50 so long as you report the loss of the card *within two business days* of discovering that it's missing. Otherwise, your liability increases to \$500 for reporting it within 60 days. If, however, you fail to report it within that 60 day period, your liability could be *unlimited*.

Once you've reported the missing/stolen ATM/debit card, you cannot be held liable for any additional charges on your account



**Checks:** If you believe any of your checks have been stolen or fraudulently used, immediately inform your bank. Have them place “stop-payment-orders” on them. Then, consider closing all existing bank accounts and opening new ones with different passwords.

Also, you should report stolen or fraudulent use of checks to:

|  |                |
|--|----------------|
| <b>Telecheck:</b>                        | (800) 710-9898 |
| <b>CheckRite:</b>                        | (800) 766-2748 |
| <b>Equifax:</b>                          | (800) 437-5120 |
| <b>ChexSystems:</b>                      | (800) 428-9623 |
| <b>International<br/>Check Services:</b> | (800) 526-5380 |
| <b>SCAN:</b>                             | (800) 262-7771 |

If you encounter trouble resolving your bank-related identity theft problems, consider contacting the agency that has jurisdiction over the institution:

**Federal Deposit Insurance Corporation  
Division of Compliance and Consumer Affairs**

550 17<sup>th</sup> Street, NW  
Washington, DC 20429  
(800) 934-3342

<http://www.fdic.gov>

(The FDIC supervises state-chartered banks that are not members of the Federal Reserve System.)

**Federal Reserve System  
Division of Consumer and Community Affairs**

Mail Stop 801  
Federal Reserve Board  
Washington, DC 20551  
(202) 452-3693

<http://www.federalreserve.gov>

**National Credit Union Administration  
Compliance Officer**

1775 Duke Street  
Alexandria, VA 22314  
(703) 518-6360

<http://www.ncua.gov> (The NCUA charters and supervises federal credit unions and insures deposits at federal credit unions and at many state credit unions.)

**Office of the Comptroller of the Currency  
Customer Assistance Group**

1301 McKinney Street, Suite 3710  
Houston, TX 77010  
(800) 613-6743

<http://www.occ.treas.gov>

(The OCC charters and supervises national banks.)

**Office of Thrift Supervision**

1700 G Street NW  
Washington, DC 20552  
(202) 906-6000

<http://www.ots.treas.gov>

(The OTS is the primary regulator of all federal and state-chartered thrift institutions including savings banks and savings and loans.)

**New York State Banking Department  
Consumer Services Division**

2 Rector Street  
New York, NY 10006  
(800) 522-3330  
<http://www.banking.state.ny.us>

(The NYS Banking Department is the primary regulator of New York State licensed financial entities including mortgage bankers, brokers and check cashers.)

**Social Security:** Where you suspect that someone has used your Social Security number to get a job, contact the Social Security Administration at (800) 772-1213 to confirm all reported earnings information. Individuals 25 or older, and not receiving benefits, will receive a Social Security statement each year. You can order a statement by submitting a request. To report fraudulent use of a Social Security number, call (800) 269-0271.

**Health Insurance:** If your health insurance card was stolen, report it to your carrier. Review your health insurance benefit statements carefully for any signs of fraud. It is possible to become a victim of health insurance fraud without your card being stolen when your insurance carrier uses your Social Security number as its identification number.



**U.S. Postal Service:** Notify the Postal Service if you believe your mail has been stolen or someone has submitted a fraudulent change-of-address form.

Write to:

## **Mail Fraud**

Chief of US Postal Inspection Service  
475 L'Enfant Plaza, S.W.  
Washington, D.C. 20260-2181

**U.S. Secret Service:** Contact the service if the crime involves counterfeit credit cards or computer hacking.

**Investments:** If you suspect that your securities' investments or brokerage accounts have been tampered with, immediately report this to your broker or manager and to the Securities and Exchange Commission.

### **SEC**

450 Fifth Street, NW  
Washington, DC 20549-0213  
(202) 942-7040 <http://www.sec.gov>

**Taxes:** Contact the Internal Revenue Service (IRS) at (800) 829-0443, if you believe that the identity thief used your identification in connection with tax violations. When you are having trouble filing tax returns call: (877) 777-4778.

**Phone Service:** To remove fraudulent phone charges from your account contact your provider or the NYS Public Service Commission (800) 342-3377 for help. The Federal Communications Commission can provide assistance on long-distance and cellular service (888)-CALL-FCC or <http://www.fcc.gov>

**Motor Vehicles:** If someone is using your identity and DMV Client ID number fraudulently or has fraudulently obtained a license or car registration in your name, contact the **New York State Department of Motor Vehicles**, License and Registration Crimes Unit Division of Field Investigations, 6 Empire State Plaza Room 431, Albany, NY 12228 or (518) 473-6464.

## **IDENTITY THEFT STATUTES**

### **FEDERAL LAW**

**Federal Identity Theft and Assumption Deterrence Act** makes it a crime to “knowingly transfer or use, without lawful authority, means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.”

The law:

- ▶ criminalizes fraud in connection with the unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents;
- ▶ subjects one who obtains anything of value aggregating to \$1000 or more during any one-year period, to a maximum fine of \$250,000 and imprisonment of up to 15 years; and,
- ▶ provides for criminal forfeiture of any personal property used or intended to be used to commit the offense and

victim assistance by the federal trade commission.

## **NEW YORK STATE LAW**

New York State law defines identify theft in the penal law and provides stiff felony penalties. The law:

- ▶ establishes criminal penalties for the unlawful, unauthorized use of identifying information, including names, addresses, driver's license numbers, social security numbers, credit card numbers, ATM codes;
- ▶ establishes specific felony and misdemeanor crimes for identity theft offenses;
- ▶ makes individuals who commit the new crime of identity theft eligible for up to 7 years in prison for the most serious form of the crime;
- ▶ enables prosecutors to focus on the root of the crime, the so-called "brokers" who compile personal information and then sell it to identity thieves;
- ▶ permits indictment of those possessing personal identifying information wrongfully taken from individuals, businesses and other entities, before that information is actually used to commit theft;
- ▶ authorizes the court to order restitution to cover a victim's costs and losses, even those associated with false information that damages a consumer's credit file;
- ▶ enables victims to sue in civil court for damages done to their credit ratings;
- ▶ authorizes eavesdropping warrants for identity theft

- crimes; and,
- ▶ allows for the prosecution of identity theft crimes in any county where the crime occurred, even if the defendant was never in that county; or in the county where the victim resided when the crime was committed; or in the county in which the person whose ID was used for a crime resided at that time of the offense.

### *IN CONCLUSION...*

In our data-driven society, there is a growing market for our personally identifiable information. As the Attorney General for the State of New York, I aggressively fight for stronger privacy protections and work closely with private businesses to encourage policies that reflect the increasing public concern for control over private and personally identifiable information.

Until stronger privacy laws are enacted, however, it is important that you consider taking precautions to ensure that your privacy is respected and that your personal data is not being used for fraudulent purposes. You can take many proactive steps to prevent important pieces of your personally identifiable information from getting into an imposter's hands.

To a large extent, privacy is up to you. You are your best protector!

Copies of this brochure and other New York State Attorney General publications are available at the Attorney General's website ([www.loag.state.ny.us](http://www.loag.state.ny.us)) or from any office listed below.

## **REGIONAL OFFICES OF THE ATTORNEY GENERAL**

### **Albany**

State Capitol  
Albany, NY 12224-0341  
(518) 474-7330

### **Binghamton**

44 Hawley Street - 17th Floor  
Binghamton, NY 13901-4433  
(607) 721-8771

### **Brooklyn**

55 Hanson Place, Suite 1080  
Brooklyn, NY 11217-1523  
(718) 722-3949

### **Buffalo**

Statler Towers  
107 Delaware Avenue  
Buffalo, NY 14202-3473  
(716) 853-8400

### **Harlem**

163 West 125th Street, Rm. 1324  
New York, NY 10027-8201  
(212) 961-4475

### **Nassau**

200 Old Country Road  
Mineola, NY 11501-4241  
(516) 248-3302

### **New York City**

120 Broadway  
New York, NY 10271-0332  
(212) 416-8000

### **Plattsburgh**

70 Clinton Street  
Plattsburgh, NY 12901-2818  
(518) 562-3282

### **Poughkeepsie**

235 Main Street - 3rd Floor  
Poughkeepsie, NY 12601-3194  
(845) 485-3900

### **Rochester**

144 Exchange Boulevard  
Rochester, NY 14614-2176  
(585) 546-7430

### **Suffolk**

300 Motor Parkway  
Hauppauge, NY 11788-5127  
(631) 231-2401

### **Syracuse**

615 Erie Boulevard West  
Suite 102  
Syracuse, NY 13204-2465  
(315) 448-4800

### **Utica**

207 Genesee St. --Rm 508

Utica, NY 13501-2812  
(315) 793-2225

**Watertown**

317 Washington Street  
Watertown, NY 13601-3744  
(315) 785-2444

**Westchester**

101 East Post Road  
White Plains, NY 10601-5008  
(914) 422-8755

**Consumer Complaint Number:**

**1-800-771-7755**

**For the Hearing Impaired:**

**1-800-788-9898**

**Visit our Website at:**

**<http://www.oag.state.ny.us>**