

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

SECURITY FREEZE INFORMATION

Any consumer in Illinois may place a security freeze on his or her credit report by requesting one in writing by certified mail to the credit reporting agency. The credit reporting agency is not allowed to charge a fee to senior citizens 65 years of age and older and victims for placing, removing for a specific time period or specific party, or removing a security freeze on a credit report. To prove you are a victim, you must also send a valid copy of a police report, investigative report, or a complaint to a law enforcement agency about unlawful use of your personal information by another person. However, for non-victims and non-seniors, a charge of \$10 will be applied for each placing, removing or temporary lifting of a security freeze. A security freeze shall prohibit, with certain specific exceptions, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer.



1470
WMBD

Listen to "Wayne and the
'Hot' Finance Lady"
Every Sunday morning from 8-10 AM

(embarrassing title, but I didn't pick the name....it's radio !)

hear a replay of every show
right from my website <http://www.FinanceLady.net>

To obtain more detailed information on how to place a security freeze on your credit reports, see below.

HOW TO "FREEZE" YOUR CREDIT FILES

A security freeze means that your file cannot be shared with potential creditors. A security freeze can help prevent identity theft. Most businesses will not open credit accounts without first checking a consumer's credit history. If your credit files are frozen, even someone who has your name and Social Security number probably would not be able to obtain credit in your name.

How do I place a security freeze?

To place a freeze, you must write to each of the three credit bureaus. Credit bureaus charge a \$10 fee to place or remove a security freeze, unless you provide proof that you are a victim of identity theft or are at least 65 years old, in which case there is no fee. A copy of your police report, investigative report or a complaint to a law enforcement agency concerning identity theft must be provided to show that you are a victim of identity theft.

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

Write to all three addresses below and include the information that follows:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze

P.O. Box 6790
Fullerton, CA 92834-6790

For each, you must:

- Send a letter by certified mail;
- If you are a victim of identity theft, you must include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.) address, Social Security number, and date of birth;
- If you have moved in the past 5 years, supply the addresses where you have lived over the prior 5 years.
- Provide proof of current address such as a current utility bill or phone bill
- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If applicable, include payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

How long does it take for a security freeze to be in effect?

After five (5) business days from receiving your letter, the credit reporting agencies listed above will place a freeze providing credit reports to potential creditors.
10 business days from receiving your letter to place a freeze on your account, the credit reporting agencies will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place.

Can I open new credit accounts if my files are frozen?

Yes. You can have a security freeze lifted for a temporary period of time. This is done at no charge for victims and seniors who are at least 65 years old. For non-victims, however, there is a \$10 charge for either temporarily lifting the security freeze or allowing a specific creditor to access your credit report.

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

The steps to do so are as follows:

- Contact the credit reporting agencies above.
- The manner by which you contact them is determined by them, but it may be by way of telephone, fax or over the Internet or by mail;
- You must provide proper identification;
- You must provide your unique PIN or password;
- And, you must include during what time period your credit report will be accessible (for example August 1 to August 5,) or include which party you want the security freeze lifted (for example: Sears.)

How long does it take for a security freeze to be lifted?

Credit bureaus must lift a freeze no later than three (3) business days from receiving your request.

What will a creditor who requests my file see if it is frozen?

A creditor will see a message or a code indicating the file is frozen.

Can a creditor get my credit score if my file is frozen?

No. A creditor who requests your file from one of the three credit bureaus will only get a message or a code indicating that the file is frozen.

Can I order my own credit report if my file is frozen?

Yes.

Can anyone see my credit file if it is frozen?

When you have a security freeze on your credit file, certain entities still have access to it. Your report can still be released to your existing creditors or to collection agencies acting on their own behalf. They can use it to review or collect on your account. Other creditors may also use your information to make offers of credit. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

Do I have to freeze my file with all three credit bureaus?

Yes. Different credit issuers may use different credit bureaus. If you want to stop your credit file from being viewed, you must freeze it with Equifax, Experian, and Trans Union.

Will a freeze lower my credit score?

No.

Can an employer do a background check on my credit file?

No. You would have to lift the freeze to allow a background check, just as you would to apply for credit. The process for lifting the freeze is described above.

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

Does freezing my file mean that I won't receive pre-approved credit offers?

No. You can stop the pre-approved credit offers by calling 888-5OPTOUT (888-567-8688). Or you can do this online at www.optoutprescreen.com. This will stop most of the offers, the ones that go through the credit bureaus. It's good for five years or you can make it permanent.

What law requires security freezes?

The Illinois security freeze law is 815 ILCS 505/2MM.

THIS FACT SHEET IS FOR INFORMATIONAL PURPOSES AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE OR AS THE POLICY OF THE STATE OF ILLINOIS. IF YOU WANT ADVICE ON A PARTICULAR CASE, YOU SHOULD CONSULT AN ATTORNEY OR OTHER EXPERT. THE FACT SHEET MAY BE COPIED, IF (1) THE MEANING OF THE COPIED TEXT IS NOT CHANGED OR MISREPRESENTED, (2) CREDIT IS GIVEN TO THE OFFICE OF THE ILLINOIS ATTORNEY GENERAL, AND (3) ALL COPIES ARE DISTRIBUTED FREE OF CHARGE.

Before using these template letters, please read the entire document for complete information.

SAMPLE FREEZE LETTER TO EQUIFAX

Date

Equifax
Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Dear Equifax:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one of the following:

I have included a \$10 fee to place a security freeze on my credit file

OR

I am a senior (at least 65 years old) and the fee does not apply to me.

OR

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

I am identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours Truly,
Your Name.

SAMPLE FREEZE LETTER TO TRANS UNION

Date

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

Dear Trans Union:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one of the following:

I have included a \$10 fee to place a security freeze on my credit file

OR

I am a senior (at least 65 years old) and the fee does not apply to me.

OR

I am identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours Truly,
Your name

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

SAMPLE FREEZE LETTER TO EXPERIAN

Date

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Dear Experian:

I would like to place a security freeze on my credit file.

My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one of the following:

I have included a \$10 fee to place a security freeze on my credit file

OR

I am a senior (at least 65 years old) and the fee does not apply to me. +

OR

I am identity theft victim and a copy of my police report (or other investigative report or complaint to a law enforcement agency concerning identity theft) regarding identity theft is enclosed.

Yours Truly,
Your name

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

IDENTITY THEFT

In order to better protect yourself, it is helpful to know some of the ways identity thefts can occur.

Thieves WILL:

- Steal wallets and purses containing personal identification and credit/bank cards.
- Steal mail, including bank and credit card statements, pre-approved credit offers, new checks and tax information
- Complete a change of address form to divert mail to another location.
- Rummage through trash, or the trash of businesses, for personal data in a practice known as “dumpster diving”
- Find personal information in homes
- Use personal information individuals share on the Internet
- Send e-mail posing as legitimate companies or government agencies with which individuals do business.
- Get information from the workplace in a practice known as “business record theft” by stealing files out of offices where a person is a customer, employee, patient or student, bribing an employee who has access to personal files, or “hacking” into electronic files.

HOW TO AVOID IDENTITY THEFT

All consumers should take the following steps to prevent identity theft from occurring:

- Review Credit Reports from each of the three major credit bureaus once a year.
- Place passwords on your credit card, bank and phone accounts.
- Secure personal information in your home.
- Ask about information security procedures in your workplace.
- Don't carry your social security card with you; leave it in a secure place.
- Don't give out your social security number unless it is absolutely necessary; ask to use other types of identifiers when possible.

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

- Don't give out personal information over the phone, through the mail or over the internet unless you have initiated the contact or are sure you know with whom you are dealing.
- Guard your mail and trash from theft.
- Destroy offers of credit received in the mail that you do not respond to; you may choose to opt-out of receiving free offers of credit.
- Carry only the identification information and the number of credit/debit cards that you actually need.
- Pay attention to your billing cycles—follow up with creditors if bills do not arrive on time.
- Be wary of promotional scams.
- Keep your purse or wallet in a safe place at work.
- Notify your credit card company if you are planning to travel out of state.

WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT

If you are a victim of identity theft, or believe you may be a victim, it is important that you take the following steps:

- Place a fraud alert on your credit reports and review your credit reports
- Place a security freeze on your credit reports.
- Close any accounts that have been tampered with or opened fraudulently.
- File a police report and ask for a copy for your records
- File a complaint with the Federal Trade Commission and the Attorney General's Office.
- Write down the name of anyone you talk to, what s/he told you, and the date of the conversation.
- Follow-up in writing with all contacts you have made about the identity theft on the phone or in person.
Use certified mail, return receipt requested, for all correspondence regarding identity theft.
- Keep all copies of all correspondence or forms relating to identity theft.
- Keep the originals of supporting documentation, like police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe the problem is resolved. If it happens again, you will be glad you did.

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

World Privacy Forum's Top Ten Opt Outs

As privacy experts, we are frequently asked about “opting out,” and which opt outs we think are the most important. This list is a distillation of ideas for opting out that the World Privacy Forum has developed over the years from responding to those questions. The list below does not contain all opt outs that are available. Rather, it contains the opt outs that we believe are the most important and will be the most useful to the most consumers.

Many people have told us that they think opting out is confusing. We agree. Opting out can range from the not-too-difficult (the FTC’s Do Not Call list is a fairly simple opt out) to the challenging (the National Advertising Initiative opt out can be tricky). Our hope is that this list will clarify which opt out does what, and how to go about opting out.

In this list, some opt outs can be done by phone, some have to be sent in a letter via postal mail, and some can be accomplished online. Some opt outs last forever, some have time limits, and others can be changed at will. If an opt out is on this list, it is because we thought it might be important enough to be worth whatever annoyance it may pose.

Not every opt out is right for everyone, and not everyone will necessarily want to opt out. It is a personal choice. Take a look at the list below, and see if any of the opt outs appeal to you, or might make a difference to you in some way. And if you know of an opt out that has been important to you that we didn’t include here, please send us your personal “top opt outs.” We’ll consider them for the next revision of this list.

Top ten opt outs:

- 1. National Do Not Call Registry**
- 2. Prescreened offers of credit and insurance**
- 3. DMA opt outs**
- 4. Financial institution opt outs**
- 5. CAN SPAM**
- 6. Credit freeze**
- 7. FERPA**
- 8. Data broker opt outs**
- 9. Internet portal opt outs**
- 10. NAI opt out**

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

1. National Do Not Call Registry (good for five years)

What it does:

The National Do Not Call Registry is a national list of phone numbers that telemarketers are not supposed to call.

If you put your home phone number on this list, telemarketers are not supposed to call you. The Federal Trade Commission manages the Do Not Call Registry. Home and mobile numbers can be on the Do Not Call list, but you can't opt out a phone at your place of business (unless you work from home using your home phone number.) Also, the Do Not Call opt out does not stop you from being called by anyone you have done business with in the last 18 months. If you make an inquiry of a merchant, the merchant can call you for six months. Charities and politicians are not covered by the Do Not Call list rules.

How to opt out:

You can opt out by phone (call *from* the number you want to get opted out) or you can opt out online. We prefer the phone opt out, not the online service. To opt out online you must provide an email address for verification, and your email address will be kept and can be shared with other federal, state, or local agencies "for any regulatory, compliance, or law enforcement purpose."

- Opt out by phone: Call 1-888-382-1222
- Opt out by TTY: 1-866-290-4236
- Opt out online: <https://www.donotcall.gov/default.aspx>

More about the Do Not Call List:

See the FTC info page: <http://www.ftc.gov/donotcall>

2. Opt out of prescreened offers of credit and insurance (five years or permanently, at your choice)

What it does:

Opting out of prescreened offers will stop you from receiving offers for credit and insurance.

Prescreened (sometimes also called "preapproved" or "prequalified") offers come in one of two ways from credit reporting files maintained by credit bureaus:

1. A creditor or insurer may ask a credit bureau for a list of consumers who meet certain criteria, for example, a minimum credit score.

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

2. A creditor or insurer may submit a list of names to a credit bureau to screen for consumers who meet certain criteria.

The result of the opt out is that you will not receive prescreened credit card or insurance offers. Many of these offers come in the mail. If you do not want these offers, or if you are concerned about someone else picking up your prescreened offers, you may want to opt out. If you do want the offers or don't receive many, you may not find this opt out important.

How to opt out:

(Note: you will be asked to give your Social Security Number to complete this opt-out.)

- Opt out by Phone: 1-888-5OptOut (1-888-567-8688). This is an automated phone system. You will have three choices: you can remove your name for 5 years, add your name back in, or permanently remove your name. When you call in, you will be asked to verify and provide some information such as your name and home phone number. You will also be asked for your Social Security Number.
- Opt out online: <https://www.optoutprescreen.com/?rf=t> Note: If you have previously opted out of pre-screened offers, you can also opt back in through this web site.

More about opting out of pre-screened offers of credit:

See FTC Privacy Choices for your Financial Information:

<http://www.ftc.gov/bcp/online/pubs/credit/privchoices.shtm#whatstop>

See FTC Prescreened Offers of Credit and Insurance page:

<http://www.ftc.gov/bcp/online/pubs/credit/prescreen.shtm>

See FDIC Financial Privacy page: <http://www.fdic.gov/consumers/privacy/faqs/index.html>

See Privacy Rights Clearinghouse: <http://www.privacyrights.org/ar/FTC-OptOutPrescreen.htm>

3. Direct Marketing Association Opt out Services (DMA opt outs)

What it does:

The DMA is the largest U.S. association of marketers – invoking DMA opt outs can diminish receiving marketing mail and catalogs.

Only businesses that are members of the DMA will comply with an opt out request through the DMA programs. The DMA offers several flavors of opt outs. It offers a Mail Preference Service opt out, an email list opt out, and an opt out that lets you remove the names of deceased people from mailing lists. The Mail Preference Service should not affect your receipt of mail and catalogs from companies that you already do business with.

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

How to opt out:

You can opt out of the DMA lists by visiting the DMA web site. One of the lists requires a \$1.00 fee if you mail in the opt out via postal mail.

- **Mail Preference Service**, usable by anyone. This list reduces mail such as catalogs, etc. It also gets your name off of some prospect mailing lists. Online form: <https://www.dmaconsumers.org/onlineform.php>. If you use the DMA online form, opting out is free. If you opt out via postal mail, you have to send a \$1.00 check.
- **Email List Opt out**. This list will get you off of some mailing lists and may help reduce some unwanted commercial email. Online form: <http://www.dmachoice.org/EMPS/>. Good for five years. This list will not act as a total cure for spam.
- **Deceased Do Not Contact List**. By signing up for this list, you will remove the names of deceased individuals from marketing lists. Online form:

https://www.ims-dm.com/cgi/ddnc_form.php.

There is no fee for the list, but you will be asked for a credit card number to verify your identity.

- **DMA Do Not Contact Service for Caregivers**: For those seeking to remove the names of individuals in their care from commercial marketing lists. Online form: <https://www.ims-dm.com/cgi/dncc.php>.

More about DMA opt outs:

If you opted out and are still getting mail or email from DMA members, you can file a complaint with the DMA by emailing them at privacypromise@the-dma.org. However, remember that it can sometimes take one month or more until putting in an opt out will have an effect, depending on the type of list. Be patient.

See information about all DMA lists: https://www.dmachoice.org/MPS/mps_consumer_description.php

See Information about the DMA mailing list, detailed:

https://www.dmachoice.org/MPS/mps_consumer_description.php?reg=C#how_to.

4. Bank/Financial Institutions opt out (This section applies to banks, credit card companies, brokerage firms, insurance companies, and other financial institutions.)

What it does:

If you opt out, you limit the extent to which a financial institution can provide your personal financial information to non-affiliates.

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

The financial institution opt outs are among the most important to understand, but they can also be challenging to understand. If you don't opt out, the assumption is that the financial institution can share your data in some circumstances. To quote from the FDIC:

Unless you opt out, your financial company can provide your personal financial information (for example, information on the kinds of stores you shop at, how much you borrow, your account balances, or the dollar value of your assets) to non-affiliates for marketing and other purposes. (FDIC Privacy Choices page, <http://www.fdic.gov/consumers/privacy/privacychoices/index.html#yourright>)

A non-affiliate is generally defined as a company that is unrelated to your financial company. The FDIC notes that a non-affiliate may include "Service providers, joint marketers--companies that have an agreement with your financial company to offer you other financial products or services, or other third-party non-affiliates--which could include companies that may want access to your financial company's mailing list to tell you about other products and services." (FDIC Privacy Choices page.)

There is a great degree of variability between financial institutions. Some do not share customer information with non-affiliates, so they do not offer an opt out. Some take an extra step and offer customers the ability to opt out of both unaffiliated and affiliated marketing. Because the type of available opt outs vary from institution to institution, you will need to read the privacy notice closely. Financial institutions are required to provide privacy notices. These notices can sometimes be difficult to understand. The opt outs are controlled in part by the Gramm-Leach-Bliley Act, a federal law that provides some privacy protections for customers of financial institutions.

How to opt out:

You may have received a privacy notice in the mail from your bank or other financial institution. If you missed it, simply ask for a copy of the company's privacy notice. They are required to have one. The privacy notice may also be posted on the financial institution's web site. Read the notice closely, and follow the company's directions for opting out. You can opt out at any time. By law, you are required to opt out in the way the financial institution determines you should, whether by letter or phone or online. We have not listed all financial institutions here, just some of the largest.

- **Bank of America:**

Opt out online: <https://www6.bankofamerica.com/privacy/Preferences.do>
Opt out by phone: 1.888.341.5000.

- **Citibank:**

No online opt out found. <http://www.citibank.com/us/d.htm> and click on *privacy* for more information
Opt out by phone: 1-888-214-0017

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

- **Chase:**

Opt out online:

https://chaseonline.chase.com/colappmgr/colportal/prospect? nfpb=true& pageLabel=page_ecarepre fs

Opt out by phone: 1-888-868-8618

- **Wachovia:**

Opt out online: https://www.wachovia.com/personal/forms/privacy_optout

Opt out by phone: 1-866-203-5722

- **Wells Fargo:**

No online opt out found. Info at https://www.wellsfargo.com/privacy_security/privacy/individuals

Opt out by phone: 1-888-528-8460

More about financial institution opt outs:

See FDIC's Your Rights To Financial Privacy Page, includes information about opt outs:

<http://www.fdic.gov/consumers/privacy/yourrights/index.html>

See FTC's Privacy Choices for your Personal Financial Information:

<http://www.ftc.gov/bcp/online/pubs/credit/privchoices.shtm>

See FDIC's Privacy Choices page, this page has an excellent section on opt out:

<http://www.fdic.gov/consumers/privacy/privacychoices/index.html#yourright>

See FDIC's Financial Privacy Page FAQ: <http://www.fdic.gov/consumers/privacy/faqs/index.html>

See Privacy Rights Clearinghouse How to Read Opt Out Notices page:

<http://www.privacyrights.org/fs/fs24a-optout.htm>.

5. Use the CAN-SPAM Opt out

What it does:

The federal CAN-SPAM Act requires that a commercial emailer give each email recipient an opt out method.

A commercial emailer must provide a return email address or another Internet-based response mechanism that allows a recipient to ask the emailer not to send future email messages to the recipient's email address. The law requires that commercial email be identified as an advertisement and include the sender's valid physical postal address. The message must contain a clear and conspicuous notice that the message is an advertisement or solicitation and that the recipient can opt out of receiving more commercial email. It also must include a valid physical postal address.

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

The federal spam law doesn't work very well to deter most spam. However, any legitimate company using email for advertising is likely to comply. If you receive an email from someone you recognize as a legitimate company and it has an opt out, you can stop that company from emailing you again. This is a very powerful tool because it flatly prohibits more commercial email from that sender to your email address.

How to opt out:

Check to make sure the email is a CAN-SPAM compliant email. Some emails offer opt outs, but the opt outs are fake. How to tell the difference?

- First, a CAN-SPAM compliant email will be labeled as an advertisement.
- Second, it will include a valid postal address for the sender.
- Third, it will include a workable opt out link of some type.

If all three elements are present in the email, then there is at least a chance that the opt out is offered in good faith. You have to use your own judgment about each email. Transactional emails are not required to offer an opt out. For example, if you place an online order with an Internet merchant, the message confirming your order, informing you of the shipping date, etc., need not offer an opt out. But if you get a message a month later announcing a sale, that commercial email should include an opt out.

More information about CAN SPAM:

See the FTC CAN SPAM page <http://www.ftc.gov/bcp/online/pubs/buspubs/canspam.shtm>.

6. Credit Freeze (also Security Freeze)

What it does:

A credit freeze (sometimes called a security freeze) lets you stop the disclosure of your credit report by a credit bureau.

The result of a credit freeze should be that neither you nor anyone else can open a new credit account in your name. (A freeze will *not* stop your existing credit cards from working.) A credit freeze can also prevent insurance companies or employers from obtaining your credit data. That's why if you are actively seeking new employment or insurance, you may want to think carefully about enacting a credit freeze unless you are currently a victim of identity theft.

The credit freeze is widely considered by consumer and privacy advocates as a potent measure to prevent some forms of identity theft. A credit freeze can be especially helpful to individuals who are having persistent problems with identity theft. Credit freeze is not for everyone, and not everyone has the right at this point to set a credit freeze.

The way a credit freeze works is that access to your consumer credit report and your credit score are locked when you put a freeze on the files. A lender or merchant will normally not issue new credit if it cannot access your credit report or score. The benefit of a freeze is that you can stop thieves from getting credit in

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

your name. The downside is that you are also stopped from getting credit unless you “thaw” the freeze. You can unlock your security freeze by using a PIN to unlock access to the credit file. Some states require the “thaw” to take no longer than 15 minutes. Some allow longer times.

The ability to freeze your credit is available nationwide through the credit reporting bureaus. There is some variability in cost and details state-by-state due to variance in state law. (For information about which states have a freeze law, see “More about credit freeze” below.)

How to opt out:

Here are two ways to find out how to opt out for your state:

- 1. The [World Privacy Forum’s Credit Freeze page](http://www.worldprivacyforum.org/creditfreeze.html) has a list of states that either have a credit freeze law, or have passed a law. Each state links to the official state information page about how to place a credit freeze, or to another information source for that state. Many of the official state information pages are excellent, and provide tips and sample letters. Even if you are not in a state with a law, as of Nov. 1, 2007, you can still set a security freeze.
<http://www.worldprivacyforum.org/creditfreeze.html>
- 2. Consumer’s Union has an excellent and frequently updated page on all current state freeze laws and requirements, with a link on how to opt out for each state and sample letters.
http://www.consumersunion.org/campaigns/learn_more/003484indiv.html

More about credit freeze:

See the FTC Credit Freeze page: <http://www.ftc.gov/bcp/edu/microsites/idtheft/credit-freeze.html>

See Consumer’s Union frequently updated page on all current state freeze laws and requirements, with a link on how to opt out for each state and sample letters.

http://www.consumersunion.org/campaigns/learn_more/003484indiv.html

See the PIRG state freeze page: <http://www.pirg.org/consumer/credit/statelaws.htm> Links to the state laws.

See California Office of Privacy Protection. Even if you don’t live in California, this is an excellent page to learn more about how credit freeze works. If you are a California resident, you will find sample letters ready for you to print out. <http://www.privacy.ca.gov/sheets/cis10securityfreeze.htm>

7. FERPA opt out (students)

What it does:

The FERPA opt out stops schools from releasing student directory information (Name, home address, date of birth, and other information) without consent, with some limitations.

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

FERPA stands for Family Educational Rights and Privacy Act. If you are a K-12 student or a college student, or the parent or guardian of a student under 18, you should know about the FERPA opt out. While some parts of school records may be given out only with written consent, schools still have the right to give out what is called "directory information" without student consent, including potentially giving the information out over the phone.

Directory information includes the student's name, school and permanent address, school and permanent home telephone number, school mail box address, major, dates of attendance, degree(s) received and dates of conferral, and other personally identifying information. There is some variability; some schools also consider the weight and height of athletes, the school email address, and participation in officially recognized activities to be directory information.

If there is a FERPA opt out form on file for the student, the student can prevent the public disclosure of his or her directory information. Then, only legitimate employers or law enforcement professionals or others with a legitimate interest should be able to access that sensitive directory information. Victims of domestic violence may find filing a FERPA opt out to be crucial to them.

How to opt out:

FERPA opt outs are often done with a FERPA form supplied by the school. Usually school records offices will have FERPA information for you, or will know where to send you to find that information. Colleges and some other schools may post the form online. For students under 18, parents have to sign the FERPA forms. This will limit how students' home address and other directory information can be released.

If you search the web for "FERPA" plus the name of your school, you may find detailed information about how to file a FERPA opt out for your school available online. FERPA opt outs may also be called "Restriction of Directory Information" at some schools.

More about FERPA opt outs:

See the U.S. Department of Education's FERPA site:

<http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html> You can find more information about FERPA here, and you can find information about filing a complaint if you have opted out of FERPA and you believe the school violated the opt out.

See the World Privacy Forum FERPA tips for jobseekers:

<http://www.worldprivacyforum.org/resumedatabaseprivacytips.html> Scroll to tip #8.

8. Data Broker opt outs

What it does:

Some commercial data brokers allow some categories of consumers to opt out of some limited uses and disclosures of personal information.

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

Commercial data brokers acquire, purchase, accumulate, and sell information about consumers. Many data brokers have large data files with some information on most Americans. The data brokers have multiple lines of business that use consumer data in different ways. Data brokers offer some very limited opt outs, and not all data brokers offer opt outs. If you are a victim of identity theft, a law enforcement professional, or a victim of domestic violence, the opt outs may be important for you. Opt out policies can be challenging to find on the data broker sites. If these links below are stale, please let us know and we will locate the new links for you.

We have mixed views on data broker opt outs. On the one hand, we think that a consumer who opts out does a good thing by exercising those few options that are available. Each consumer opting out helps to preserve opt outs for all consumers. However, the data broker opt outs are generally quite limited, and it is nearly impossible to tell just what effect an opt out will actually have. When you read the opt out offerings carefully, you will see that they are often qualified. Consumers who are victims of identity thieves, victims of domestic violence, public officials, and others may have the greatest interest in seeking what opt out options are available.

How to opt out:

Note: of the data brokers in this list, Acxiom, Choicepoint, and Lexis Nexis are the largest. If you are an identity theft victim, a law enforcement professional, or have a strong safety need to opt out of data broker databases, start with these three companies first.

- **Acxiom:**

You can opt out of some of Acxiom's marketing and directory products. To do this you will need to request an opt out by sending an e-mail to optoutus@acxiom.com or by calling 1-877-774-2094. You can read more about Acxiom opt outs at <http://www.acxiom.com/default.aspx?ID=2851&DisplayID=18>

- **Choicepoint:**

You can opt out of some of Choicepoint products, with limitations.

All consumers can opt out of the Choicepoint Marketing database. To opt out, go to Choicepoint's online form at http://www.privacyatchoicepoint.com/optout_ext.html#optout and then fill out the form.

Some consumers can opt out of other Choicepoint products. Here is what Choicepoint says about this particular opt out:

Certain states allow their public and elected officials to prohibit dissemination of certain public records. In addition, ChoicePoint may allow public and elected officials, including law enforcement officers, to opt out of certain PFG products and services in cases where the official is working undercover, on a high-profile assignment, or under threat of death or serious bodily harm. Public and elected officials must submit their opt out requests, in writing on official government letterhead, to: ChoicePoint Inc. Office of Privacy Compliance 1000 Alderman Drive MD 71-A Alpharetta, GA

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

30005 Email: privacy@choicepoint.com Also, ChoicePoint may allow certain private individuals who are facing a substantial risk of physical harm or who are victims of Identity Theft to opt out of certain PFG products and services. Individuals who may qualify for this opt out must submit their request, in writing. Such requests must include documentation substantiating the risk of physical harm or the individual's status as an Identity Theft victim. Accepted documentation must include a properly filed police report, or a letter from a law enforcement agency, or a law enforcement contact familiar with the issue necessitating the request. Requests must be submitted to: ChoicePoint Inc. Office of Privacy Compliance 1000 Alderman Drive MD 71-A Alpharetta, GA 30005 Email: privacy@choicepoint.com For more on Choicepoint optouts, see http://www.privacyatchoicepoint.com/optout_ext.html#optout

- **Intelius:**

This company's opt out policy is difficult to evaluate. They say they will opt you out as a "courtesy," "temporarily." We do not know exactly what either courtesy opt out or temporarily specifically means, or how long exactly this opt out will last. Nevertheless, to opt out, go to <http://find.intelius.com/privacy-faq.php#5> . Intelius directs consumers to fax or mail their name and address as it appears on its website to opt out.

Intelius fax number: (425) 974-6194

Intelius mailing address: Intelius, Inc. Attn: CUSTOMER SERVICE 500 – 108th Ave NE #1660 Bellevue, WA 98004

- **Lexis Nexis:**

If you fall under three categories, you can opt out of some Lexis Nexis non-public information databases. (These categories include you if you are a state, local or federal law enforcement officer or public official and your position exposes you to a threat of death or serious bodily harm; or you are a victim of identity theft; or you are at risk of physical harm.) There is a detailed process for you to go through to opt out. If you are a victim of identity theft or have been the victim of domestic violence, this opt out could be helpful.

See this web site for the Lexis Nexis process:

<http://www.lexisnexis.com/terms/privacy/data/remove.asp>.

- **US Search Profile Opt Out:**

You can opt out of part of the US Search record profile. Specifically, you can opt out of information culled from non-public record sources. An example of this is information compiled from magazine subscriptions – many people do not realize that magazine subscription information is often available for sale through data brokers, mailing list vendors, and others.

If you would like to opt out, you will need to mail in a signed request with the following information - your full name, e-mail address, mailing address, social security number, date of birth, past addresses and aliases to: US SEARCH, Opt out Program 600 Corporate Pointe, Suite 220 Culver City, CA 90230.

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

More on US Search opt out:

<http://www.ussearch.com/consumer/commerce/about/privacy.jsp;jsessionid=0WgYmX6nG96xwxsPoXhG9A**.node4?adID=10002101>

More about data broker opt outs:

See the Privacy Rights Clearinghouse Info Brokers Opt Out page:

<http://www.privacyrights.org/ar/infobrokers-optout.htm>

See the CDT Opt Out Site: <http://optout.cdt.org/> The CDT Opt out site was last updated in 2002, but it is still useful.

9. Internet Portal Opt Outs

What it does:

Some large Internet portals allow some limited forms of opt outs. These opt outs can have varying effects, for example, some opt outs spare you from receiving unwanted email.

How to opt out:

We have not listed every portal that you could potentially opt out from This is a selection of opt-outs that some large Internet portals offer.

- **Amazon:**

Find out about choices at <http://amazon.com/gp/help/customer/display.html/102-6769060-6468131?ie=UTF8&nodeId=468496#choices>. There is a Customer Communications Preferences link at <http://amazon.com/gp/gss/ccp/>. Note, you will need to sign in before seeing this page.

- **Ebay:**

After you have signed in to your Ebay account, you can make choices by finding the *Preferences* link under *My Account*.

- **MSN:**

At the MSN.com site, click on the MSN privacy link at the bottom of the main screen. Then look for *Communications Preferences*. You will be offered a series of links that allow you to exercise choice about the types of communications that you will receive.

- **Yahoo:**

Sign in to your Yahoo account and look for the *Options* Link. Click on that link and then click on *YAHOO! Delivers*. You can then select or unselect what types of advertising email that you want by

****SPECIAL REPORT****

PROTECTING YOUR IDENTITY

checking or unchecking boxes with descriptions. Note: if you don't uncheck the boxes, all boxes will be automatically selected, so watch this closely.

More about Internet portal opt outs:

We encourage you to read the privacy policies of Internet web portals. The opt outs can make a difference, and one of the best ways to find out about the opt outs that are available to you is to read the privacy policy for that web site.

10. Network Advertising Initiative opt out (NAI opt out)

What it does:

The Network Advertising Initiative (NAI) offers a centralized opt out system that allows Internet users to avoid some types of tracking of their web activities.

Some online ads appear on multiple web sites -- these ads are generally called network ads. If you browse with cookies turned on (as many people do) at a couple or more of web sites with network ads, or make some purchases or register at those sites, then your activities may in some situations be tracked. In some cases, things you do online can be linked back to you personally by name or email address and then merged with other information about you.

If you opt out of NAI tracking, it means that companies that have tracking ads at multiple web sites will no longer assemble a file of all of the places you have visited, will no longer link your web activities with you personally, and will no longer merge the web activities connected with their ads with other information about you. This is how the NAI describes it:

While advertising networks do collect data on consumers who view their advertising, this data is often anonymous. However, profiles derived from tracking consumers' activities on the Web can be linked or merged with "personally identifiable information" (PII). It can also be combined with offline purchase data or information collected via a survey, census, or registration form. These activities are most often invisible to consumers. (<http://www.networkadvertising.org/consumer/faqs.asp>)

The NAI opt out uses what is called an "opt out cookie" to tell advertisers not to track you. This opt-out can seem counter-intuitive: you accept a cookie on your computer to make sure you aren't tracked using cookies.

How to opt out:

- **Step one:** You must accept third party cookies for this opt out to work. Open your web browser and check the cookie settings to accept all cookies.
- **Step two:** Open the following page: http://networkadvertising.org/consumer/opt_out.asp. You will see a prominent *Consumer Opt Out* button. After you click this button you will see an opt out page listing network advertisers with a checkbox next to each. This page is supposed to allow you to check and uncheck boxes, then click a button and automatically opt you out of all NAI tracking. In our tests of the opt out system, we found that the page can exhibit variable results based on the system used to

****SPECIAL REPORT****
PROTECTING YOUR IDENTITY

access it, and does not always function at 100 percent for all systems, or at least it did not in our tests. Using computers running Firefox or IE on MS Windows and Safari on Mac OSX, our tests found that only some of the checked boxes successfully opted out. (The page has a feature that will tell you whether the opt out was successful or not.) Using a computer running Mozilla on a SUN Ultra, and computer running Firefox on Mac OSX, our tests found that all boxes did opt out.

- **Step three:** If the page did not automatically opt you out of everything you wanted to opt out of, you can follow the individual links listed under each advertiser on the NAI opt out page. You may have to click through a number of pages before you can actually opt out. The NAI provides a phone number and an email for you to call if you are having trouble opting out: phone 207-351-1500, x110 or send an email to membership@networkadvertising.org.
- **Note:** After you have opted out, if you remove the opt out cookies from your computer, the opt out must be repeated. We reiterate: this opt out may be helpful and useful, but it also can be challenging.

More about the NAI opt out:

See the NAI Frequently Asked Questions Page: <http://www.networkadvertising.org/consumer/faqs.asp>

See World Privacy Forum cookie page: <http://www.worldprivacyforum.org/cookieoptout.html>

This information is not legal advice, and should not be used in lieu of legal advice.

Authors: Pam Dixon and Robert Gellman

Document history:

Updated January 28, 2008, November 5, 2007, August 6, 2007. Originally posted July 22, 2007