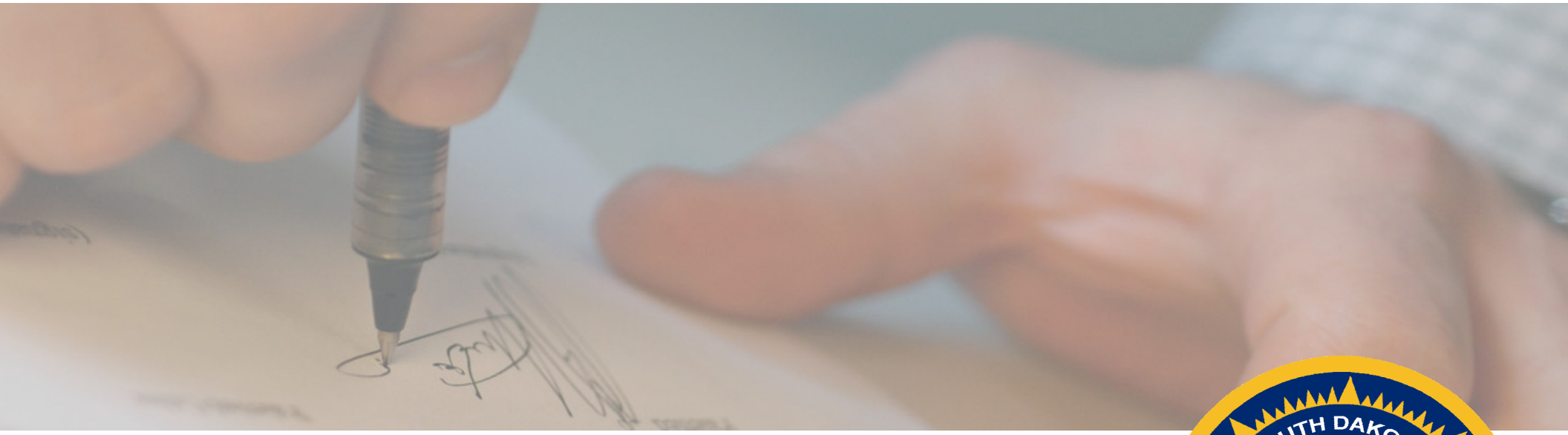
Privacy Rights



Office of Attorney General • Division of Consumer Protection

1.800.300.1986 (in-state)

A letter from South Dakota Attorney General

Marty J. Jackley

Dear South Dakotans,

Thank you for your interest in our handbook designed to assist you in protecting your privacy. Unfortunately your personal privacy is lost, unknowingly forfeited, purchased or stolen every day. This includes more than your name, address and social security number. It includes other things such as your shopping habits, driving record, medical diagnoses, credit score and much more. It can happen in every day situations like donating to a charity, visiting the doctor's office, surfing the internet, joining an organization, or paying your mortgage. The right to privacy is oftentimes taken for granted. But for anyone who has been the victim of identity theft, this lost privacy can mean financial loss as well as months or years of dealing with loss of credit, calls from harassing debt collectors, police, credit bureaus, businesses and government agencies.

As Attorney General of South Dakota, I believe it imperative for our citizens to take whatever steps available in protecting their personal and financial privacy. This handbook was developed to educate and assist you in taking these steps.

I hope you find the information in this book useful. If you have questions or would like additional information, please contact my office by calling 1-800-300-1986 or logging on to our website at www.state.sd.us/atg.

Very truly yours,

Marty Jackley
Attorney General

TABLE OF CONTENTS

PRIVACY RIGHTS

FINANCIAL PRIVACY: What you can do to protect yourself

Our economy generates an enormous amount of data. Most users of that information are from honest businesses - getting and giving legitimate information. Despite the benefits of the information age, some consumers may want to limit the amount of personal information they share.

When your personal information is sold or gets into circulation, it poses two threats: you will receive more unwanted solicitations – and/or you could become the victim of "identity theft" such as someone opening an account using your name. Control your personal information – especially your credit cards, bank accounts, and Social Security Number (SSN).

The information contained in this brochure will explain some of your rights and the ways in which you can protect your financial privacy.

IDENTITY THEFT

Every day you share personal information about yourself with others. It's so routine that you may not even realize you're doing it. You may write a check at the grocery store, charge tickets to the ball game, rent a car, mail your tax returns, schedule a doctor's appointment or apply for a credit card. Each transaction requires you to share personal information such as:

- Bank and credit card account numbers
- Income
- Social Security Number (SSN)
- Name, address and phone numbers

There are unscrupulous individuals, like identity thieves, who want your information to commit fraud.

Identity theft occurs when someone uses your personal identifying information, like your name, SSN, or bank or credit card number, without your permission, to commit fraud or other crimes. The crime takes many forms. Identity thieves may rent an apartment, obtain a credit card, or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make—or until you're contacted by a debt collector.

Identity theft is serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for educations, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

ID Theft & Privacy Rights: Tips to Remember

- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.

- Do not give out personal information on the phone, through the mail or over the internet unless you have initiated the contact and know whom you are dealing with. Identity thieves may pose as representatives of banks, internet service providers, and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers, and other identifying information. Legitimate organizations with which you do business have the information they need and will not ask you for it. This activity performed by identity thieves is called **phishing**, as they are "fishing" for your personal information.

- Put passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number. Also, do not use obvious choices like a series of consecutive numbers.

- Minimize the identification information and the number of cards you carry. Don't put all your Personal Identification Numbers (PIN) or similar information in one compartment in your purse, briefcase or backpack. Never keep the PIN information and the credit or bank account cards in the same location.

- Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help or have service work done in your home. Also, shred or destroy such documents as receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements, expired charge cards, and credit offers you get in the mail. This will help stop any identity thief who may pick through your trash to capture your personal information.

- Notify your credit card company if you plan to travel out of state.
- Find out who has access to your personal information at work and verify that the records are kept in a secure location.
- Read the privacy policy on all websites directed to children. Websites directed to children or that knowingly collect information from kids under 13 must post a notice of their information collection practices.
- Consider ordering a copy of your credit report from each of the three major credit reporting agencies every year. Make sure it's accurate and includes only those activities you've authorized.
- Don't carry your social security card with you. Leave it in a secure place.
- Keep a list or photocopy of all your credit cards, account numbers, expiration dates, and telephone number of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditor in case your cards are lost or stolen. Do the same with your bank accounts.

DID YOU KNOW

Use a secure browser when shopping online to guard the security of your transactions. When submitting your purchase information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

FREE CREDIT REPORTS

Your credit report contains information about where you live, how you pay your bills, and whether you've been sued or arrested, or have filed for bankruptcy. Credit reporting agencies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy and privacy of information in the files of the nation's credit reporting agencies`.

Monitoring your credit card statements and your credit reports are the most important steps you can take to safeguard your credit and financial identity.

An amendment to the federal Fair Credit Reporting Act, known as the Fair and Accurate Credit Transaction Act, established a **FREE** credit report program. The program requires the three national credit reporting agencies, Equifax, Experian and TransUnion, to provide consumers, upon request, with a free copy of the credit report every 12 months. It is crucial that you check for inaccuracies and fraudulent use of your accounts. The free reports are available only through a central site set up by the three agencies.

To obtain the free reports, consumers can:

- Order online at www.annualcreditreport.com
- Call 1-877-322-8228 (mailed within 15 days of receipt but allow 2-3 weeks for delivery)
- Complete the Annual Credit Report Request form, available at www.ftc.gov/credit and mail to:

  Annual Credit Report Request Service
  PO Box 105281
  Atlanta GA 30348-5281

We recommend that you stagger your reports and order one every 4 months. Staggering the requests throughout the year would allow for a continual watch of the credit history and provide further protection from incidences of identity theft. So — if you order from only one company today you can still order from the other two companies at a later date.

NOTE: Your credit score is NOT included with the free credit report offered by Annual Credit Report.

SAMPLE LETTER ON NEXT PAGE

The following information is required to process your request. Omission of any information may delay your request.

Once complete, ***mail certified*** **to:**

Annual Credit Report Request Service, PO Box 105281, Atlanta GA 30348-5281

Social Security Number: _____

Date of Birth: _____

FIRST, MIDDLE & LAST NAME: _____

(List all name variations, including Jr, Sr, II, etc.)

CURRENT MAILING ADDRESS: _____

_____

_____

PREVIOUS MAILING ADDRESS: _____

(Fill in your previous mailing address if you have moved in the last 2 years) _____

_____

I WANT A CREDIT REPORT FROM: (Shade Each that you would like to receive)

- ☐ Equifax
- ☐ Experian
- ☐ TransUnion

SHADE HERE IF, FOR SECURITY REASONS, YOU WANT YOUR CREDIT REPORT TO INCLUDE NO MORE THAN THE LAST FOUR DIGITS OF YOUR SOCIAL SECURITY NUMBER. ☐

If additional information is needed to process your request, the consumer credit reporting company will contact you by mail.

Your request will be processed within 15 days of receipt and then mailed to you.

The last page of this brochure has a check-off form to use when you order.

Sample Annual Credit Report Letter

IF YOU HAVE NEGATIVE INFORMATION

When negative information in your report is accurate, only the passage of time can assure its removal. A consumer reporting company can report most accurate negative information for seven (7) years and bankruptcy information for ten (10) years. Information about an unpaid judgment against you can be reported for seven (7) years or until the statute of limitations runs out, whichever is longer. There is no time limit on reporting: information about criminal convictions; information reported in response to your application for a job that pays more than $75,000 a year; and information reported because you've applied for more than $150,000 worth of credit or life insurance. There is a standard method for calculating the seven (7) year reporting period. Generally, the period runs from the date that the event took place.

DID YOU KNOW

You need to provide your name, address, Social Security Number, and date of birth when requesting your credit report. Also, if you have moved in the last two years, you may have to provide your previous address. To maintain the security of your file, each nationwide consumer reporting company may ask you for some information that only you would know, like the amount of your monthly mortgage payment. Each company may ask you for different information because the information each has in your file may come from different sources.

CORRECTING CREDIT REPORT ERRORS

Under the FCRA, both the credit reporting agency and the information provider (that is, the person, company, or organization that provides information about you to a credit reporting agency) are responsible for correcting inaccurate or incomplete information in your report. To take advantage of all your rights under this law, contact the agency and the information provider.

Step One

Tell the credit reporting agency, in writing, what information you think is inaccurate. Include copies (NOT originals) of documents that support your position. In addition to providing your complete name and address, your letter should clearly identify each item in your report you dispute, state the facts and explain why you dispute the information, and request that it be removed or corrected. You may want to enclose a copy of your report with the items in question circled. Your letter may look something like the sample on page 11. Send your letter by certified mail, “return receipt requested,” so you can document what the credit reporting agency received. Keep copies of your dispute letter and enclosures.

Reporting companies must investigate the items in question — usually within 30 days — unless they consider your dispute frivolous. They also must forward all the relevant data you provide about the inaccuracy to the organization that provided the information. After the information provider receives notice of a dispute from the credit reporting agency, it must investigate, review the relevant information, and report the results back to the agency. If the information provider finds the disputed information is inaccurate, it must notify all three (3) nationwide credit reporting agencies so they can correct the information in your file.

When the investigation is complete, the credit reporting agency must give you the results in writing and a free copy of your report if the dispute results in a change. This free report does not count as your annual free report. If an item is changed or deleted, the agency cannot put the disputed information back in your file unless the information provider verifies that it is accurate and complete. The consumer reporting company also must send you a written notice that includes the name, address, and phone number of the information provider.

If you ask, the credit reporting agencies must send notices of any corrections to anyone who received your report in the past six months. You can have a corrected copy of your report sent to anyone who received a copy during the past two years for employment purposes.

If an investigation doesn’t resolve your dispute with the credit reporting agency, you can ask that a statement of the dispute be included in your file and in future reports. You also can ask the agency to provide your statement to anyone who received a copy of your report in the recent past. **You can expect to pay a fee for this service.**

Step Two

Tell the creditor or other information provider, in writing, that you dispute an item. Be sure to include copies (NOT originals) of documents that support your position. Many providers specify an address for disputes. If the provider reports the item to a credit reporting agency, it must include a notice of your dispute. And if you are correct — that is, if the information is found to be inaccurate — the information provider may not report it again.

DID YOU KNOW

The law allows you to order one free copy of your credit report from each of the nationwide credit reporting agencies every year.

ADDING ACCOUNTS TO YOUR REPORT

Your credit file may not reflect all your credit accounts. Although most national department store and all-purpose bank credit card accounts will be included in your file, not all creditors supply information to credit reporting agencies: some local retailers, credit unions, and travel, entertainment, and gasoline card companies are among the creditors that don't.

If you've been told that you were denied credit because of an "insufficient credit file" or "no credit file" and you have accounts with creditors that don't appear in your credit file, ask the credit reporting agencies to add this information to future reports. Although they are not required to do so, many credit reporting agencies will add verifiable accounts for a fee. However, understand that if these creditors do not report to the agency on a regular basis, the added items will not be updated in your file.

Sample Dispute Letter

Date
Your Name
Your Address
City, State, Zip Code

Complaint Department
Name of Company
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. I have circled the items I dispute on the attached copy of the report I received.

This item *(identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)* is *(inaccurate/incomplete)* because *(describe what is inaccurate or incomplete and why)*. I am requesting that the item be removed *(or request another specific change)* to correct the information.

Enclosed are copies of *(use this sentence if applicable and describe any enclosed documentation, such as payment records and court documents)* supporting my position. Please reinvestigate this *(these)* matter(s) and (*delete or correct*) the disputed item(s) as soon as possible.

Sincerely,

Your name

Enclosures: *(List what you are enclosing)*

OPT-OUT

Our economy generates an enormous amount of data. Most users of that information are from honest businesses getting and giving legitimate information. Despite the benefits of the information age, some consumers may want to limit the amount of personal information they share.

Marketing Opt-Out: Many organizations are offering consumers choices about how their personal information is used. For example, many feature an “opt-out” choice that limits the information shared with others or used for promotional purposes. When you ”opt-out,” you may cut down on the number of unsolicited telemarketing calls, promotional mail and spam e-mails that you receive. Look for ways to “opt-out” of mailing lists to reduce “junk” mail and unauthorized solicitations. Many mail order forms, magazines and marketers now provide a box to check if you do not want your name(s), address and shopping habits to be shared with other companies.

What Opt-Out Means: The term "opt-out" means that *unless* and *until* you inform your bank, credit card company, insurance company, or brokerage firm that you do not want them to share or sell your customer data to other companies, they are free to do so.

Financial Privacy Opt-Out: Federal privacy laws give you the right to stop (opt-out of) some sharing of your personal financial information. These laws balance your right to privacy with the financial companies' need to provide information for normal business purposes.

Protect Your Financial Privacy: To protect your **financial privacy**, tell your financial companies that they may not sell or share your customer data with other companies. Federal law requires banks, credit card companies, insurance companies, and brokerage firms to send you a privacy notice each year. If you opt-out, you limit the extent to which the company can provide your personal information to non-affiliates. If you do not opt-out within a "reasonable period of time" — generally about 30 days after the company mails the notice — then the company is free to share certain personal financial information. If you didn't opt-out the first time you received a privacy notice from a financial company, it's not too late. You can always change your mind and opt-out of certain information sharing. Contact your financial company and ask for instructions on how to opt-out. Remember, however, that any personal financial information that was shared before you opted-out cannot be retrieved.

Pay attention to the mail you receive from your bank, insurance company, credit card company, and brokerage firm. Look for words such as "*Privacy Notice*," "*Privacy Policy*," and "*Opt-Out Notice*." You might receive such notices via e-mail or the company's website if that is the way you normally do business with them.

OPT-OUT: Pre-Approved Offers of Credit

The three (3) major credit reporting agencies offer a toll-free number that enables you to "opt-out" of having pre-screened credit offers sent to you. By calling **1-888-5-OPTOUT (567-8688)** or visiting www.optoutprescreen.com, your name will be removed from the mailing list for five (5) years. Your request is shared with all three credit reporting agencies.

In addition, you can instruct the agencies to not share your personal information for promotional purposes, which is an important step towards eliminating unsolicited mail. To prevent your personal information from being shared, send a letter, call or e-mail to each of the credit reporting agencies.

Make sure to send your opt-out letter to all three (3) major credit reporting agencies.

SAMPLE LETTER ON NEXT PAGE

Sample Opt-Out Letter for Credit Reporting Agency

EQUIFAX, INC.
Options
PO Box 740123
Atlanta GA 30374-0123

EXPERIAN
Consumer Opt-Out
701 Experian Pkwy
Allen TX 57013

TRANSUNION
Marketing List Opt-Out
PO Box 97328
Jackson MS 39288-7328

Date

To whom it may concern,

I request to have my name removed from your marketing lists. Here is the information you have asked me to include in my request.

FIRST, MIDDLE & LAST NAME:
(List all name variations, including Jr, Sr, II, etc.)
_____
_____

CURRENT MAILING ADDRESS:
_____
_____
_____

PREVIOUS MAILING ADDRESS:
(Fill in your previous mailing address if you have moved in the last 6 months.)
_____
_____
_____

SOCIAL SECURITY NUMBER:
_____
DATE OF BIRTH:
_____

Thank you for your prompt handling of my request.

_____
SIGNATURE

SOCIAL SECURITY NUMBER & PRIVACY

Be very protective of your **Social Security Number** (SSN). Only provide it when you know it is required (tax forms, employment records, most banking, stock and property transactions). If the SSN is requested by a government agency, look for the Privacy Act notice. This tells you if your SSN is required, what will be done with it, and what happens if you refuse to provide it.

Give your SSN only when absolutely necessary, and ask to use other types of identifiers. If your SSN is your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your SSN as your policy number. Your employer and financial institutions need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your SSN for general record keeping.

Pay attention to your **Social Security Statement of Earnings and Benefits**. The Social Security Administration mails your Statement each year about three (3) months before your birthday. Your Statement contains a record of your earning history and an estimate of how much you and your employer paid in Social Security taxes. It also includes estimates of benefits you (and your family) may be eligible for now and in the future. If you need to order your Statement at another time, call (800) 772-1213 for instructions. Web: www.socialsecurity.gov.

BE ASSERTIVE

If someone requests your Social Security Number, ask:

- How will it be used?
- Why do you need it?
- How do you protect if from being stolen?
- What will happen if I don't give it to you?

SOCIAL SECURITY NUMBER

There is no law that prevents businesses from requesting your SSN. If you don't provide it, some businesses may not provide you with the service or benefit you want. Unfortunately, your credit report, bank account and other financial records are linked to your social security number. If your social security number falls into the hands of the wrong person, you could be the victim of credit or banking fraud. Ask if you can use an alternate number such as your driver's license number. You may need to be assertive and persistent. Do not have your SSN printed on your checks. It is too easily available to persons.

Social Security Number
Theft and Misuse

The Social Security Administration Office of the Inspector General investigates cases of identity theft. Report allegations that a SSN has been stolen or misused by contacting the Social Security Administration at:

Social Security Administration Fraud Hotline

PO Box 17768

Baltimore MD 21235

1-800-269-0271

www.ssa.gov

DO NOT CALL REGISTRY

Consumers can also choose to have their name included in the National Do Not Call Registry. You can register for free at www.sddonotcall.com or by calling 1-888-382-1222 (you must call this number from the phone on which you receive the unwanted calls). Once your number is on the Do Not Call Registry, telemarketers will be on notice that you do not want telemarketing calls. **Note:** You may also place your cell phone on the registry by calling the toll-free number from your cell phone.

Placing your number on the National Do Not Call Registry will stop most, but not all telemarketing calls. You may still receive calls from political organizations, charities, telephone surveyors or companies with which you have an existing business relationship with over the last twelve (12) months. You can also receive calls in an attempt to collect a debt or contract. Calls can also be made for the purpose of obtaining information, and establishing a date, and time for an appointment which will take place at the solicitor's place of business, or the consumer's home. These types of calls CANNOT be made by an automated telephone dialing system.

The last page of this brochure has a check-off form to use when you register.

Telemarketing Sales Rule – Request Not To Call

If you don't put your number on the national registry, you still can prohibit individual telemarketers from calling, by asking each to put you on their company's do not call list. By law they have to honor your request. If you have an established business relationship with a company, you still can ask them not to call you. The company must honor your request at that point.

NOTE: Although callers soliciting charitable contributions do not have to search the national registry, a for-profit telemarketer calling on behalf of a charitable organization must honor your request not to receive calls on behalf of that charity.

Complaints regarding calls that are exempt from the National Do Not Call Registry should be reported to the Attorney General's Division of Consumer Protection at 605-773-4400 or 800-300-1986 (in-state only).

DIRECT MARKETERS

The Direct Marketing Association offers the mail and e-mail Preference Services, which allow you to opt-out of receiving direct mail marketing for **five (5)** years, and unsolicited commercial e-mails from many national companies for **one (1)** year.

When you register with these services, your name will be put on a "delete" file that is updated four times a year and made available to direct-mail marketers. Two to three months after your name is entered into the quarterly file, you should notice a decrease in the number of solicitations you receive. However, your registration will not stop mailings from organizations NOT registered with DMA's Mail Services.

FOR MAIL:
To have your name deleted from many direct mailing lists, write to the Direct Marketing Association and tell them to put you on their opt-out lists. Include the name(s) and addresses of household members who do not want to receive unsolicited mail.

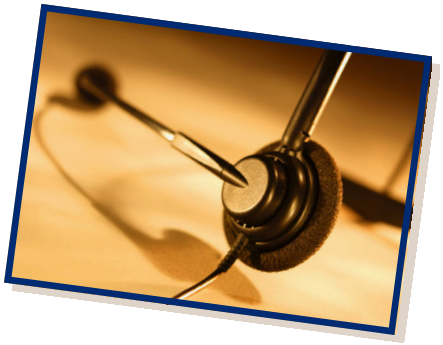
Direct Marketing Association
Mail Preference Service
PO Box 643
Carmel NY 10512
www.dmaconsumers.org/consumerassistance.html

FOR E-MAIL:
To opt-out of receiving unsolicited commercial e-mail, use the Direct Marketing Association's online form at www.dmaconsumers.org/offemaillist.html. Your online request will remain effective for **one (1)** year.

MARKETING & SOLICITATIONS

Junk Mail—Telemarketing

In general, be aware that when you provide your name, address, phone number and other personal information, your name could end up on mailing lists. The following activities often result in "junk" mail and telemarketing calls:



- Filling out warranty and product registration cards. Give only your name, address and information about the product you purchased. Leave the rest blank.
- Joining or donating money to clubs, organizations, charities. Tell them in writing not to sell or exchange your name with other groups.
- Subscribing to magazines, book clubs and music/CD clubs. Tell them not to sell your name.

- Listing your phone number and address in the phone book. Omit your address, or be unlisted.
- Avoid entering **sweepstakes** and other contests if you want to stay off mailing and telemarketing lists aimed at "opportunity seekers," often called "sucker lists." The purpose of contests is to compile names and addresses that can be sold to marketers for other solicitations, such as fundraising or catalog offers. Some contests and special offers are scams, especially those that ask you for money up front or which offer get-rich-quick schemes.
- Remember, many prize promotions or drawings are geared to gather your personal information. Often times, you are giving them permission to call or solicit you in the future.

SECURITY BREACHES

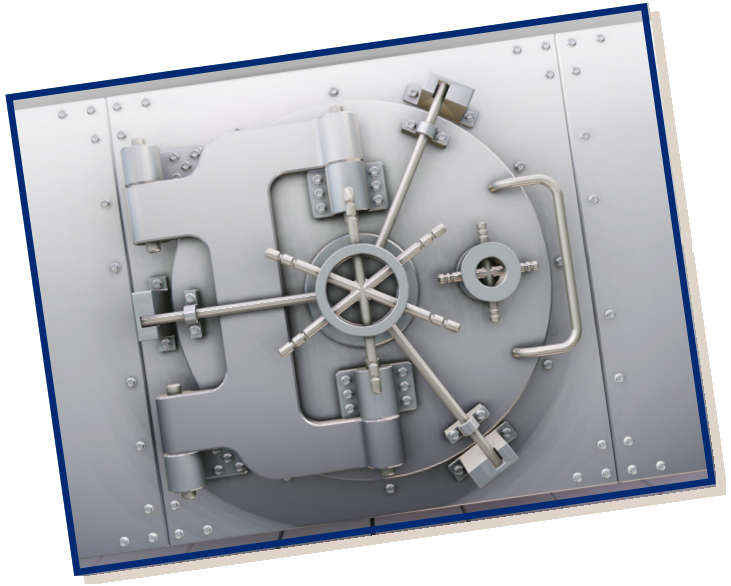
Have you received a letter informing you that your personal information may have gotten into the wrong hands?

It is increasingly common for companies, educational institutions, and government agencies — whether or not their state has a breach notice law — to notify individuals when computer files containing personal information have been hacked, stolen, or lost. If the file includes your SSN, financial account numbers, driver's license numbers — in short, data that would be useful to identity thieves — there are steps you can take to reduce your risk of fraud.

So, what should you do if you receive a letter telling you that your personal information has been compromised? First, don't panic. A security breach does not necessarily mean that you will become a victim of identity theft.

1. **Figure out what type of breach has occurred.** Has a breach occurred with your *existing* financial account? Has your SSN been compromised, with the chance that *new accounts* can be established by an imposter? Has your driver's license number been compromised, or another government-issued ID document?

    - **Existing accounts** : If the breach involved your *existing* credit or debit card account, you will want to monitor your monthly account statements very carefully. Contact the creditor if your statement does not arrive on time. A missing bill could mean that an identity thief has changed your address. Check statements for transactions you did not make. Dispute those fraudulent charges directly with the credit or debit card company. The company will likely cancel the account and give you a new card and account number. You will not be responsible for the fraudulent charges if you properly dispute them. It's very important to report the fraudulent transactions immediately. In some situations, the financial company will not wait for evidence of fraud. It will instead cancel the existing account and issue a new account number right away.



- **The potential for new accounts to be opened** : If the breach involved disclosure of your SSN, a fraudster could use that information to open *new accounts* in your name. You will not immediately know of the new accounts because criminals usually use an address other than your own for the account. Since you will not be receiving the monthly account statements, you are likely to be unaware of the account(s). That is why it is so important to place a fraud alert with the three credit reporting agencies immediately when you learn that your SSN has been compromised, and then to monitor your credit reports on an ongoing basis. Other evidence of new account fraud include receiving credit cards in the mail that you did not apply for, being denied credit when you know you've had a good credit score, and being contacted by debt collectors for payments that you do not owe.

- **ID Documents:** Nearly all the security breaches reported to date have potentially involved financial accounts. But if you are notified of a breach involving your driver's license or another government document, contact the agency that issued the document and find out what it recommends in such situations. You might be instructed to cancel the document and obtain a replacement, or the agency might instead "flag" your file to prevent an imposter from getting a license in your name.

2. **For security breach situations involving your Social Security Number (SSN) —** in other words, breaches in which there is an opportunity for *new* accounts to be opened in your name you should consider taking the following actions:

    - **Notify the credit reporting agencies and establish a fraud alert.** Immediately call the fraud department of one of the three credit reporting agencies — Experian, Equifax, or TransUnion. As soon as the agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.
    - **Order your credit reports.** If you are a victim of identity theft, you will see evidence of it on your credit report. Surveys have found that the sooner individuals learn of the identity theft, the more quickly they can clean up their credit reports and regain their financial health.
    - **Examine your credit reports carefully**. When you receive your credit reports, look for signs of fraud such as credit accounts that are not yours. Check if there are numerous inquiries on your credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on your credit report for each of those attempts. Usually identity thieves do not succeed in opening all of the accounts that they apply for, only some. Multiple inquiries that you yourself have not generated are a sign of potential fraud. Also, check that your SSN, address(es), phone number(s), and employment information are correct.
    - **If your credit report indicates you are a victim of identity theft, you will want to immediately take steps to remove the fraudulent accounts**. If you are a victim you may contact the Federal Trade Commission or the SD Office of Attorney General website for step-by-step information on what you should do.
- **Continue to monitor your credit reports.** *Be aware that these measures may not entirely stop new fraudulent accounts*

from being opened by an imposter. Credit issuers do not always pay attention to fraud alerts. Once you have received the first free copy of your credit report, follow up in a few months and order another.

- **Consider a security freeze.** The three credit reporting agencies — Equifax, Experian, and TransUnion, offer security freezes nationwide. Read on for further information. (Please note that it this would only apply to new credit accounts).

FRAUD ALERTS AND SECURITY FREEZES

Security Freezes are a much better defense against ID theft. This explains the differences.

Fraud Alerts: Anyone can ask the three major credit reporting agencies to place a fraud alert on their credit reports. A fraud alert is simply a statement on your credit report that you may be a victim of fraud. Consumers can obtain a 90-day fraud alert if they believe they've been victimized.

Consumers who can provide evidence they've been victimized, such as a police report, can get an extended fraud alert that lasts up to seven years. A fraud alert directs lenders to verify an individual's identity before issuing loans or credit, typically by calling the individual first. Fraud alerts are supposed to alert you when someone applies for credit in your name and signals creditors to contact you for permission to issue credit in your name. Creditors, however, aren't required to abide by or even check the alert. Accounts can still be opened in your name even if you have a fraud alert on your credit report.

When you request a fraud alert from one agency, it will notify the other two for you. Your credit file will be flagged with a statement that says you may be a victim of fraud and that creditors should phone you before extending credit.

- Equifax fraud department: (888) 766-0008 • Web: www.equifax.com
- Experian fraud department: (888) EXPERIAN (888-397-3742) • Web: www.experian.com/fraud
- TransUnion fraud department (800) 680-7289 • Web: www.transunion.com

Security Freezes: A Security Freeze provides much stronger protection than a Fraud Alert. With a security freeze, no one can open any form of credit in your name without the correct **Personal Identification Number (PIN)** supplied by you. Your credit file is off limits to potential lenders, insurers and even potential employers. A security freeze means that your credit file cannot be shared with potential creditors, insurance companies or employers doing background checks without your permission. Most businesses will not open credit accounts without checking a consumer's credit history first. A security freeze means that your credit file cannot be shared with potential creditors or potential identity thieves.

A security freeze can help prevent identity theft because even someone who has your name, address and SSN probably would not be able to obtain credit in your name. This, however, does not mean that you won't be able to get credit for yourself or allow potential employers to run a background check. The three (3) credit reporting agencies assign a PIN for you when you freeze your report. Using this PIN, you can lift the freeze when necessary. With a credit lock-down, a criminal can have your name, birthday and SSN — but it won't matter. No credit will be issued. To obtain more detailed information on how to place a security freeze on your credit reports, see below.

HOW TO "FREEZE" YOUR CREDIT FILES

How do I place a security freeze?
To place a freeze, you must request a security freeze in writing by **certified mail** to each of the three credit reporting agencies. If you are a victim of identity theft there is no cost for the placing, temporarily lifting (also referred to as "thawed") or removing a security freeze, as long as you have a report from either the police or a law enforcement agency. South Dakota residents who are not identity theft victims must pay $10 to freeze each credit report, or a total of $30 to freeze their files with the three (3) credit reporting agencies. There is also a $10 fee to temporarily lift (also known as "thaw") or permanently remove a security freeze on their credit report.

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

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834-6790

You must:

- Send a letter by certified mail.
- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, SSN, 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 showing your name and current mailing address.

- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc).
- If you are a victim of identity theft, to avoid the fee you must include a copy of report of alleged identity fraud or an identity theft passport.
- Pay the $10 fee by check, money order, or credit card (Visa, Master Card, American Express or Discover cards only.) Give name of credit card, account number and expiration date and Card Identification Number (4-digit number on front of American Express or 3-digit number on back of other credit cards).

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 previously will place a freeze providing credit reports to potential creditors. After ten (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 or password.
Keep this PIN or password in a safe place.

How long will credit report remain frozen?
It will automatically expire seven (7) years from the date of placement and then can be renewed.

Can I change my mind, once I place the security freeze?
Yes. To permanently remove a security freeze, you must request it along with your 10-digit PIN and two (2) forms of identification (e.g. pay stub with address and utility bill). It will cost $10 with each credit reporting agency to remove it.

Can I open new credit accounts if my files are frozen?
Yes. You may have a security freeze lifted for a specific date range (e.g. March 15-March 21) or provide proper information regarding the third party you want to receive your credit report. There will be a $10 fee to each credit reporting agency in doing so. The steps you are to take are as follows:

- Contact the credit reporting agencies mentioned in this section.
- The manner by which you contact them is determined by them.
- You must provide proper identification.
- You must provide your unique PIN or password.
- If you are requesting to open your credit for a specific period of time, you must provide during what time period your credit report will be accessible.
- If you are requesting to open your credit to a specific party, you must specify who that party is.

How long does it take for a security freeze to be lifted?
Credit reporting agencies must life 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.

What law requires security freezes? South Dakota Codified Law 54-15 became effective on July 1, 2006.

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 reporting agencies 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 have access for collecting child support payments, or taxes, or for investigating Medicaid fraud. 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 reporting agencies?
Yes. Different credit issuers may use different agencies. If you want to stop your credit file from being viewed, you must freeze it with Equifax, Experian, and TransUnion.

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 previously.

To protect my credit, does my spouse's credit file have to be frozen too?
Yes. Both spouses have to freeze their separate credit files, via separate letters requesting the freeze, in order to get the benefit. That means the total cost for freezing is $10 X 3 credit reporting agencies x 2 people = $60.

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 reporting agencies. It's good for five (5) years or you can make it permanent.

(Opt-Out Information can be found on pages 12-15 in this handbook)

Sample Letter: Request for Security Freeze

Send a separate letter requesting a security freeze to each consumer reporting agency. Make sure to write clearly and sign the letter. Send the letter certified mail-keep a copy for your records. Enclose a copy of the required documents-never the originals. There is not a fee for identity theft victims but you must include a copy of the police report.

Date:

[AGENCY NAME & ADDRESS]

I would like to place a security freeze on my credit file.
My name is: _____
(Be sure to include full name, middle initial, former names, & Jr./Sr./III)

My current address is:_____

In the past two years I have also lived at: (list all addresses)
_____
_____

My Social Security Number is:_____
My date of birth is: _____
As proof of identification and residence, I am enclosing a copy of the following two items:_____
[List what you are enclosing. Enclose copy of a government ID card such as driver's license or military ID AND a copy of a utility bill, phone bill or insurance or bank statement.- don't send originals]

__ I am an identity theft victim and a copy of my police report is enclosed (NO CHARGE)

OR

__ I will pay the $10 fee for placing the freeze by:
Money Order _____
Credit Card – [Visa, MasterCard, American Express or Discover]_____
Card Number_____
Expiration Date:_____
Card Id Number_____
[4-digit number on front of American Express above account number or 3-digit number on the back of other cards at the end of the account number.]

Sincerely,
[YOUR SIGNATURE AND ADDRESS]

HEALTH CARE & PRIVACY

This is a brief summary of your rights and protections under the federal health information privacy law. This is known as Health Insurance Portability & Accountability Act (HIPAA)

Your Privacy Matters

Most of us feel that our health and medical information is private and should be protected, and you have the right to know who has this information. Federal law:

- Gives you rights over your health information
- Sets rules and limits on who can look at and receive your health information

Your Health Information is Protected by Federal Law

Who must follow this law?

- Most doctors, nurses, pharmacies, hospitals, clinics, nursing homes, and many other health care providers
- Health insurance companies, HMOs, most employer group health plans
- Certain government programs that pay for health care, such as Medicare and Medicaid

What information is protected?

- Information your doctors, nurses, and other health care providers place in your medical record
- Conversations your doctor has about your care or treatment with nurses and others
- Information about you in your health insurer's computer system
- Billing information about you at your clinic
- Most other health information about you held by those who must follow this law

The Law Gives You Rights Over Your Health Information

Providers and health insurers who are required to follow this law must comply with your right to

- Ask to see and get a copy of your health records
- Have corrections added to your health information
- Receive a notice that tells you how your health information may be used and shared
- Decide if you want to give your permission before your health information can be used or shared for certain pur-

poses, such as for marketing
- Get a report on when and why your health information was shared for certain purposes
- If you believe your rights are being denied or your health information isn't being protected, you can:
  – File a complaint with your provider or health insurer
  – File a complaint with the U.S. Government — http://www.hhs.gov/ocr/hipaa

You should get to know these important rights, which help you protect your health information. You can ask your provider or health insurer questions about your rights. You also can learn more about your rights, including how to file a complaint, from the website at www.hhs.gov/ocr/hipaa/.

Your Health Information Privacy Rights

The Law Sets Rules and Limits on Who Can Look At/Receive Your Information

To make sure that your information is protected in a way that does not interfere with your health care, your information can be used and shared

- For your treatment and care coordination
- To pay doctors and hospitals for your health care and help run their businesses
- With your family, relatives, friends or others you identify who are involved with your health care or your health care bills, unless you object
- To make sure doctors give good care and nursing homes are clean and safe
- To protect the public's health, such as by reporting when the flu is in your area
- To make required reports to the police, such as reporting gunshot wound

Your health information cannot be used or shared without your written permission unless this law allows it. For example, without your authorization, your provider generally cannot

- Give your information to your employer
- Use or share your information for marketing or advertising purposes
- Share private notes about your mental health counseling sessions

MEDICAL IDENTITY THEFT

Medical identity theft occurs when someone steals your personal information (like your name, Social Security number, or Medicare number) to obtain medical care, buy drugs, obtain insurance benefits, or submit fake billings to Medicare in your name. Medical identity theft can disrupt your life, damage your credit rating, and waste taxpayer dollars. The damage can be life-threatening to you if wrong information ends up in your personal medical records.

Protect Your Personal Information

- Guard your Medicare and Social Security numbers carefully. Treat them like you would treat your credit cards or bank account numbers. Never give your Medicare number over the phone or to anyone other than your medical provider or insurance company. Legitimate government agencies typically will never ask for this for information over the phone.
- Be suspicious of anyone who offers you free medical equipment or services and then requests your Medicare number. If it's free, they don't need your number!
- Do not let anyone borrow or pay to use your Medicare ID card or your identity. It's illegal and it's not worth it!
- If your Medicare card is lost or stolen, report it right away. Call Social Security at 1-800-772-1213 (TTY 1-800-325-0778) for a replacement.

Report Medicare Fraud and Medical Identity Theft

- If you notice unusual or questionable charges, contact your health care provider. It may just be a mistake.
- If your complaint is not resolved by your provider, report the questionable charges to Medicare at 800-447-8477 or go their website at http://www.medicare.gov/.
- If you suspect your are a victim of Medical Identity Theft contact the SD Division of Consumer Protection at 800-300-1986 for further assistance.

Check All Your Medical Bills, Medicare Summary Notices, Explanation Of Benefits, and Credit Reports

- Were you charged for any medical services or equipment that you didn’t get?
- Are the services and charges correct?
- Does your credit report show any unpaid bills for medical services or equipment you didn’t receive?
- Have you received any collection notices for medical services or equipment you didn’t receive?

DEBT COLLECTORS & PRIVACY

A call from a collection agency is often the first sign of trouble for an identity theft victim. The federal Fair Debt Collection Practices Act (FDCPA) applies to debt collectors. Under the Fair and Accurate Credit Transaction Act (FACTA), if you are contacted by a collection agency about a debt that resulted from the theft of your identity, the collector must so inform the creditor. You are entitled to receive all information about this debt — such as applications, account statements, late notices from the creditor — that you would be entitled to see if the debt were actually yours. In addition, FACTA says that a creditor, once notified that the debt is the work of an identity thief, cannot sell the debt or place it for collection.

The federal Fair Debt Collection Practices Act (FDCPA) sets the national standard for collection agencies. The FDCPA, enforced by the Federal Trade Commission (FTC), prohibits abusive collection tactics that harass you or invade your privacy. Public embarrassment and the prospect that your personal information might be shared with others are real concerns when dealing with a collection agency. The FDCPA includes provisions intended to safeguard privacy.

The FDCPA says discussions about the debt can only be held with (1) the individual, (2) the creditor, (3) an attorney representing one of the parties, and (4) a credit reporting agency. Public airing of your business intended to shame you into paying a debt is not allowed.

Debt collectors:

- Cannot exchange (with other agencies) information about individuals who allegedly owe a debt.
- Cannot distribute a list of alleged debtors to its creditor subscribers.
- Cannot advertise a debt for sale.
- Cannot compile a list of debtors for sale to others.
- Cannot leave messages with third parties, asking them to have the debtor call the collector.

NOTES

FREE CREDIT REPORT CHECK-OFF LIST

Consumers are able to obtain one copy of their credit report from each of the three credit reporting agencies each year. Consumers may want to request these reports from each of the reporting agencies at the same time, or stagger the requests throughout the year.
(SEE PAGE 6 FOR MORE INFORMATION)

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

YEAR: ________

- □ Equifax — Date Ordered________
- □ Experian — Date Ordered________
- □ TransUnion — Date Ordered________

Date of Registry for:

DO NOT CALL REGISTRY

________________ (no renewal required)

OPT-OUT

Pre-Approved Credit Cards:

________________ (renew every 5 years)

Direct Marketers:

FOR MAIL:

________________ (renew every 5 years)

FOR E-MAIL:

________________ (renew every year)

SECURITY FREEZE

________________ (renew every 7 years)

South Dakota Office of Attorney General
Division of Consumer Protection
1302 E Hwy 14 Ste 3 • Pierre SD 57501
605.773.4400 • 800.300.1986 (in-state only)
605.773.7163 (fax)

2010