PROTECTING YOUR PRIVACY IN THE INFORMATION AGE

What every consumer should know about the use of individual information

acxiom

TABLE OF CONTENTS

CONCERNED ABOUT YOUR PRIVACY IN THE INFORMATION AGE? SO ARE WE.

At Acxiom, we provide consumer information to responsible companies all around the world. Obviously, we have a stake in the issue of consumer privacy. We also know, however, that consumers need certain protections—and that there is some information that should remain private and confidential.

To help you better understand this subject, we've produced this booklet. Among other things, it explains some of the ways businesses, charities, Internet sites and other organizations use the consumer information we provide. You may be surprised at all the ways information can directly and indirectly benefit you and your family. There is a lot of misinformation in the news and on the Internet about the risks posed by the uses of information about you. This booklet is intended to help you understand the benefits and the risks in today's Information Age.

Some of the terminology about privacy issues that is commonly used can be confusing. It may be helpful to review or refer to the section at the end of this booklet "Useful Terms to Understand" when you encounter a term you don't completely understand.

We've included information about how you can have your name removed from telemarketing solicitations, direct mail promotions, email marketing and set your browser to block the cookie setting that companies use to personalize your online experience on the Internet should you choose to do so. We've also included information on how to assure information about you in public sources is correct.

The Information Age brings you plenty of benefits, but also creates some new risks. The loss of your privacy doesn't have to be one of them. Acxiom believes the more informed you are about the uses of individual information, the less you have to fear—and the more you can enjoy the many advantages afforded by the appropriate use and exchange of information.

HOW CAN I PROTECT MY PRIVACY?

Although it's a surprise to many, the Information Age is not as risky as some would lead you to believe. Consumers have a number of protections routinely provided. It is important for you to learn about these protections and how to exercise the options that are offered to you.

NOTICE

Reputable companies will tell you what information they collect and maintain, how it is being used and when it is being shared with other parties. This is usually done in the form of a "Privacy Policy." You can view the privacy policy of most companies on their website or by contacting the company and asking for a copy. Companies who do not post or provide a privacy policy should be given extra scrutiny.

CHOICE

Most companies will give you some choices regarding the use and dissemination of personal information about you. Some of these choices are outlined later in this booklet. If the company provides information about you to third parties for their marketing uses, you should be given a chance to "opt-out." This means you can request the company not provide information about you to third parties for marketing purposes.

ACCESS AND ACCURACY

Organizations should maintain appropriate procedures that ensure the information they use about you for important or substantive decisions is accurate. You should be able to access such information if you feel it may not be accurate and have erroneous information corrected, updated or removed.

SECURITY

You should reasonably expect that information about you will be protected from unauthorized access and use. Organizations should maintain effective security systems to protect against such occurrences. There are a lot of reported security breaches in the news which can be concerning. More information about your risks relative to security breaches is provided in the section "Should I Worry about Security Breaches?" on page 14.

AWARENESS

There are a lot of resources available to you should you have specific concerns about your privacy. A number of sites where you can go are provided in the section "Where Can I Learn More" on pages 21-24.

WHERE DO COMPANIES GET MY NAME?

Organizations use information from a variety of sources for a variety of reasons. You are familiar with some of them—such as businesses wanting to send you an offer, better understand their marketplace, develop new products and improve customer service. In other cases, companies use information to protect you and themselves from risks related to identity fraud.

Most companies rent or buy lists of individuals who they believe are likely to be interested in their products or services. They will use these lists to market to you either offline or online. These lists come from a variety of sources, including public records, telephone directories, and from companies who exchange or rent their customer file for marketing purposes to other organizations who have a legitimate need for the information. The rental or exchange of customer files has been a common practice for decades and does not pose a security risk to you. The exchange usually involves only the basic contact information and very general information about your purchases. These lists are used to send mail to you, call you, email or text you about special promotions or offers. This enables a company to more effectively reach out to individuals who are not customers but who might have an interest in or need for their product or service.

It is also a very common practice for a business or organization to create a marketing file of names, addresses and other information related to their customers' purchases. This information may include household characteristics obtained from surveys you fill out or from general communication with you.

Marketing, however, is just one use for information about you. Early detection and prevention of fraud by verifying your identity is a second use that offers significant benefits to both you and businesses. Being able to correctly recognize a customer, especially when transacting business

over the phone, on the Internet or via a mobile device, helps reduce the chances you will become a victim of identity fraud. Identifying information is commonly shared between companies and available from information providers like Acxiom to help businesses in reducing the incidence of fraud.

There are also other uses of personal information you may not have considered, such as courts tracing parents who fail to meet child support obligations, organ, blood and bone marrow donor groups needing accurate, up-to-date information about donors, law enforcement agencies apprehending criminals, attorneys searching for missing heirs or family members looking for lost relatives, to name just a few. All of these provide significant benefits to society as a whole and are permitted, or in some cases required, by various laws such as background screening for child care centers and school bus drivers.

WHAT KIND OF INFORMATION IS AVAILABLE?

There is a variety of information available to businesses and organizations. Most of it is non-sensitive, but some of it is sensitive.

PUBLIC RECORDS

Collected primarily from state and federal government sources, information about you may come from public records, including property deeds, marriage and professional licenses, and birth and death records. Information is also available from court proceedings, voter registration files, drivers license records and motor vehicle registrations. Various federal and state laws place restrictions on the use of some of these sources.

PUBLICLY AVAILABLE INFORMATION

Some information is considered in the public domain, meaning anyone has access to it. This type of information includes telephone directory listings, professional registries, classified ads, information posted in chat rooms, on blogs and in public sections or designated as public on social network sites. Publicly available information is not always regulated by law, but responsible providers self-regulate its use through industry codes of conduct.

CUSTOMER INFORMATION

This is information that is collected when you provide information about yourself to an organization when you inquire about a product, make a donation, make a purchase, register a product warranty or receive a service. This information includes details you provide about how to contact you and a record of your interactions with the company or organization. This information is regulated in some cases by law and in other cases by industry practice. In addition to this, responsible organizations develop their own policies to assure appropriate use of the information.

SELF-REPORTED INFORMATION

Information you voluntarily provide on a survey or questionnaire is considered self-reported. When this type of information is collected, you should be informed of the intended uses and your options for said use. Both law and industry practices limit the use of this information.

PASSIVELY COLLECTED INFORMATION

The Internet and other technologies, like mobile devices with location tracking features and interactive televisions, may collect information about you, or your device, without you having to take any action. In fact in many cases you may not be aware any collection is taking place. Some of this collection is necessary to provide you a service such as recording the number of times you go through the express lane of a toll booth so you can be charged for the toll or when you've have had a car wreck and need help locating your car to send emergency assistance. It can also be used to provide you relevant advertising such as offering you a discount on a specialty coffee from a coffee shop you are near, or to provide online advertising tailored to interests that have been identified based on other websites you have recently visited or keywords you have recently used in a search. Both law and industry practices limit the use of this information.

SENSITIVE INFORMATION

Some information, if used inappropriately, can have more serious consequences. This includes your Social Security number, drivers license number, medical records, wage and salary information, tax reports, your credit report and information that personally identifies your children. Sensitive information should be kept confidential and is usually not provided to other organizations unless you give specific permission or unless it is permitted, or required, under state or federal law.

In order to develop credit reports, credit reporting agencies gather information from banks and other financial institutions with which you have a relationship. The Federal Trade Commission closely regulates the use of this information as directed by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA).

In order to assure you will be a responsible employee, tenant or insured individual, employers, landlords and insurance companies may ask your permission to do a background check on you. This involves verifying the information you provided on your application with the source of the data. Background checks can also involve obtaining a credit report if your financial situation is pertinent to the employer or landlord. The Federal Trade Commission closely regulates the uses of this information as directed by the Fair Credit Reporting Act (FCRA).

WHY DO THEY WANT TO KNOW SO MUCH ABOUT ME?

Organizations want personal information for a number of reasons, but generally they have two main purposes in mind—delivering more relevant marketing messages and reducing risk—to you and themselves.

RELEVANT MARKETING MESSAGES

To effectively market products and services to individuals and households, organizations need information about the people they're trying to reach. For example, if a business wants to offer a new product to a past customer or reward a current customer with a special discount, it needs accurate contact information to reach that customer. The business may also need household characteristics: home ownership; interests; musical/sports/hobbies/preferences; or lifestyle information, such as current retirees in the household, to deliver the right offer to the right customer.

Or the business might want to attract new customers. In this case, the business would use information indicating a previous interest in a similar product or service. The business would also like to focus their customer acquisition efforts with some household characteristics, interest and lifestyle information. They use this information to transfer the knowledge they have about existing customers' interests and needs to individuals they don't know. Informed targeted marketing reduces the chance that you receive unwanted solicitations and maximizes marketing efforts.

REDUCING RISK FOR THE ORGANIZATION AND YOU

Organizations also use information to manage risks—authenticating someone's identity, verifying information about a customer and detecting or preventing fraud. Most consumers don't think about these uses of information as they go on behind the scenes. For example, a car dealership might need to verify a buyer's identity, or a police officer might need to locate a suspect's or witness' address. All these activities require quick but secure access to information. The information used to verify someone's identity or locate them in some instances is governed by law and in other instances is governed by industry codes of conduct.

Consumers now demand real-time responses when they apply for credit, which includes mortgages, credit cards and large in-store purchases. To provide this, businesses must be able to access accurate, personal information to determine whether credit should be extended and in what amount. The FCRA governs the use of information for credit purposes.

DOES THE USE OF PERSONAL INFORMATION BENEFIT ME?

Often consumers are not aware of the many ways that the use of personal information can directly benefit them in their everyday lives. Here are just a few:

SPECIAL OFFERS

When businesses use accurate information to target their promotions, you are more likely to receive more offers that appeal to you and fewer that do not. Information enables promotions to reach the consumers for whom a product or service was designed. It also permits added benefits, such as special discounts, early-bird notices of sales, special event alerts, free trials and other frequent shopper benefits that are communicated through direct mail, email, telemarketing, online or your mobile device.

SHOPPING BY MAIL, PHONE, INTERNET, OR YOUR MOBILE DEVICE

Today's shopper can order merchandise from home or the office using a number of convenient methods, including mail, phone, the Internet or even your mobile device. Information helps make this happen. Companies use personal information to produce and distribute catalogs tailored to specific groups of individuals. The result of effective marketing produces a wider range of products and services from which consumers can choose. While you sometimes wonder why you are getting all these catalogues or emails, the vast majority of consumers find one or more of them of interest and actually do make purchases as a result of receiving them. Often they learn about new products or services that they had not known about or that were not available in their local area.

PERSONALIZING YOUR INTERNET EXPERIENCE

Many consumers shop on the Internet. While searches provide access to information you are seeking, some sites with a wide variety of content personalize the experience you have when visiting their website based on your past visits to the site. This can be in the form of recommendations, like you see on retail shopping sites, or prioritizing a long list of products based on the types of products you have bought or browsed previously. This allows you to quickly find items of interest.

FREE OR LESS COSTLY CONTENT ON THE INTERNET

Many popular Internet sites are funded through advertising, just like commercials help fund TV shows. As more people shop online, advertising there has become much more common. Just like in the offline world, advertisers want to reach individuals who have an interest or need for their product or service. In order to do this, they want to understand you better. Since you can easily browse the Internet without identifying yourself technology is used to help the advertiser better predict your level of interest in their products and services. This is most often done through the use of cookies which are placed on your browser and collect information about sites visited and searches made by your browser. In many cases this is done anonymously, but in cases where you have bought from the site, they may know who you are. This information is then summarized into interest categories and used to deliver more relevant ads.

FINDING FAMILY OR FRIENDS

Online directories offer a quick, easy—and often free—way to locate family and friends who have moved. Telephone books, alumni directories and professional membership registries are just a few examples of this helpful use of personal information.

LEGAL MATTERS

Access to personal information has made it far easier to locate people who legally need to be found: parents evading child support orders, missing heirs entitled to inheritances, pension beneficiaries and witnesses in criminal and civil matters.

REAL ESTATE TRANSACTIONS

Real estate brokers depend on property information from the county clerk's office to obtain recent sales figures of comparable properties in a neighborhood to help you buy or sell a home or investment property. The government uses this information to help accurately calculate property taxes. Mortgage companies use it to determine the value of a piece of property for loan purposes.

OBTAINING CREDIT

When you apply for credit, lenders contact credit bureaus for the information they need to determine how much credit should be extended. Highly automated systems enable them to easily check your credit report and provide a quick response. You have the right under the FACT Act to obtain a copy of your credit report annually at no cost. To maximize your credit opportunities and to ensure you are getting the lowest interest rate possible, it is important that you periodically get a copy of your report and review it. This is also a good way to be sure your information has not fallen into the hands of identity thieves.

FRAUD REDUCTION

When a consumer places an order or opens an account, businesses rely on external personal information to verify the accuracy of the information provided, thus minimizing the risk of mistakes and even fraud. They can also check shipping information to ensure the product you order is going to the correct address. This kind of verification makes it more difficult for criminals to purchase items with stolen credit cards and false identity representation.

WHAT ARE THE RISKS FROM INFORMATION EXCHANGES?

While you enjoy a lot of benefits and greater security from the exchange of information about you, there are some risks that you should be aware of and protect against. Furthermore, a lot of myths about these risks have grown over the years as concerns about identity theft and new uses of information have increased. This section is intended to clarify some of the confusion and provide practical tips for everyday use.

IDENTITY THEFT AND TAKEOVER

This is a crime that is escalating. It is also a crime that is becoming more complex. Understanding where you are at risk and what protections are available to you is important.

You or someone you know has probably had a credit card lost or stolen. In these cases, all the credit card issuers have made it very easy to remedy the situation by canceling your old card, getting a new card, and not holding you liable for charges you did not make. By law you are only liable for up to $50.00 of fraudulent charges, but most credit issuers waive this liability. If your credit card is lost or stolen, contact the issuer immediately.

If your actual identity, not just your credit card, is stolen, however, the remedy can be much more difficult and time consuming. Identity takeover is when a fraudster has enough information to impersonate you—changing the address on your credit accounts so you do not get your statement or see the fraudulent charges, opening new credit accounts in your name, or withdrawing funds from your existing accounts. Understanding a few simple tips can help you avoid the crime of identity takeover. They are provided on pages 12-14 of this booklet.

You should be aware that while identity fraud on the Internet gets a lot of news coverage, rarely do these articles distinguish between the crime of credit card theft and identity takeover. This is important because your risks are very different. You should also know that the Internet is not the most common place for either crime. The vast majority of these crimes still originate from offline loss or theft of information about you, and a significant portion of these crimes are committed by family and friends.

EMAIL AND PHONE SCAMS

While the Internet has provided a new means for scamming consumers, there have been scammers who act in person and have used the telephone for many years to get information or money from consumers for illegal purposes.

You should never provide personal information, especially sensitive information such as your Social Security number, date of birth or bank account/credit card numbers to anyone. If this information is requested, you must consider who is requesting and why it is being requested. Any business that you have already provided this sensitive information to will never contact you to request the same information again. Possibly legitimate businesses may ask you to verify a portion of this information or may ask you verifying questions to which you have already provided answers. If you still have reservations, you always have the opportunity to postpone your reply until you have confirmed with your local Better Business Bureau that they represent a legitimate business. If you have been scammed, report the incident to the authorities, credit bureaus, your financial institutions and to the Better Business Bureau so others will not be victimized.

In recent years a practice known as “phishing” has developed. This is where you receive an email that looks like it comes from a reputable business or government agency when in fact it does not. It usually directs you to a website, which also looks legitimate, where you are asked for personal and usually sensitive information such as account numbers, date of birth or your Social Security number. These emails are scams. Do not supply any of the requested information. If you are not certain of the authenticity of an email, contact the business or agency offline and verify the request. These kinds of scams should also be reported to the Federal Trade Commission and to the business or agency the email claims to represent.

In addition, many of the companies that frequently are impersonated offer resources and tips to help authenticate legitimate email from them. More information about recognizing email scams can be found in the section “Where Can I Learn More” on pages 21-24.

FINANCIAL RECORDS AND RECEIPTS

It is less and less common for bank statements and other financial records to contain personal information about you that could be used to commit identity fraud. However, it is wise to be careful. Review the statement and if it contains more than your name, address and account number, it is best to file such statements in a secure place and tear them up or shred them when you throw them away. If you live in an apartment building or other multifamily dwelling, you may be at greater risk since the trash is often more easily available to thieves. You should also protect these records from domestic help and others who have access to your home.

Several years ago, invitations to apply for credit, pre-approved offers of credit and receipts from credit card purchases contained sensitive personal information that was needed by identity thieves, including Social Security numbers and other information needed to commit identity takeover. In all these instances companies have changed their practices to protect consumers. Applications for credit and pre-approved offers no longer contain sensitive information. You may also have noticed that in most cases now only the last four digits of your credit card number is printed on the receipt. These practices have greatly reduced the ability of fraudsters to make purchases or takeover your identity with a piece of mail or a receipt.

HOW CAN I PROTECT MYSELF FROM IDENTITY FRAUD?

Criminals committing identity fraud are sophisticated. To lower your chances of becoming a victim, follow these simple steps.

DON'T CARRY SENSITIVE INFORMATION AROUND WITH YOU

Minimize the information you routinely carry that could contribute to identity theft if your wallet or purse was stolen. Do not carry your Social Security card or information with bank account numbers and associated PINs in your wallet or purse.

Keep a list or photocopy of all your credit cards, bank accounts and investments—the account number, PIN, expiration date and telephone number of the customer service—in a secure place at home (not your wallet or purse) so you can quickly contact these companies in the event of a theft or loss.

PROTECT SENSITIVE INFORMATION

Never give your Social Security number over the phone or the Internet unless you are dealing with someone you know. Do not give your credit card number or other personal information over the phone or on the Internet unless you know the company or you have initiated the call. Identity thieves have been known to call or email their victims with very real sounding but false stories to lure them into providing sensitive information.

Each year when you receive your Social Security Personal Earnings and Benefits Estimate Statement examine it for fraud. The Social Security Administration mails it to adult age SSN holders about three months before your birthday. The SSA website has additional information. Information on how to reach them is provided on page 22.

CHECKING YOUR CREDIT REPORT

If you have reason to believe you are a victim of credit card fraud or identity takeover, you can get a free copy of your credit report, and you can also order one free copy annually even if you do not suspect any problems. Information on how to request a copy of your credit report is provided on page 23. In addition, several companies, including the three credit bureaus, offer credit monitoring services for an annual fee. These services notify you when there is any activity on your credit report, thus alerting you to possible fraud. The websites and toll-free numbers are provided on pages 21-24.

PROTECT YOUR MAIL

Install a locked mailbox at your residence, use a Post Office™ box or commercial mailbox service to deter mail theft. When you are away from home for an extended time, have your mail held at the Post Office or ask a trusted neighbor to pick it up. Be sure to watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive within a reasonable timeframe.

If your regular bank or other financial statement is late, contact the business and inquire about the late statement. When you pay bills, do not leave the envelopes with checks in an unsecured mailbox for the carrier to pick up. If stolen, your checks can be altered and then cashed by the imposter.

PASSWORDS AND PINS

When creating passwords and PINs (personal identification numbers), do not use factual information about you such as the last four digits of your Social Security number, mother's maiden name, your birthdate, middle name, pet's name, consecutive numbers or other facts that could easily be discovered by thieves. It is best to create random passwords that combine letters and numbers, even though these are harder to remember. Do not write down your passwords and keep them near your computer or visible on your desk.

INTERNET AND COMPUTER SAFEGUARDS

Install a firewall on your home computer to prevent hackers from obtaining access to your computer if you connect to the Internet by DSL or cable modem.

Install and update virus protection software to prevent a worm or virus from causing your computer to send out files or other stored information.

Protect files that contain sensitive personal data, such as financial account information, with passwords. Create passwords that combine six to eight numbers and letters, both upper and lower case—the longer the password the better.

Before disposing of your computer, remove data by using a strong "wipe" utility program. Do not rely on the "delete" function to remove files containing sensitive information.

SHOULD I WORRY ABOUT SECURITY BREACHES?

Because of new laws, when a company experiences a security breach various requirements must be followed to notify federal agencies, law enforcement and consumers who had information involved in the breach. You may have received a letter from a company, academic institution or government agency about a breach involving information about you.

The good news is that research shows that even though there appears to be an increase in the number of breaches, there does not appear to be an increase in identity takeovers as a result of breaches. This does not mean that you are not at risk. Instead, it means that you do not need to be increasingly concerned.

If you receive a letter, pay close attention to what was lost or stolen. If it involved your credit card information, you are at much less risk than if it involved your Social Security number, birth date, or other information that could contribute to an identity takeover.

HOW CAN I PREVENT UNWANTED CALLS FROM TELEMARKETERS?

People sometimes feel they are powerless to prevent intrusive calls by telemarketers. However, you have a number of options to limit or eliminate these calls.

FEDERAL TRADE COMMISSION'S "DO-NOT-CALL" REGISTRY

If you do not wish to receive any calls from businesses with whom you do not have an existing relationship, put your telephone number on the Federal Trade Commission's "Do-Not-Call" registry. The toll-free number and website are provided on page 21.

UNWANTED SOLICITATIONS TO YOUR CELL PHONE

As more people rely on their cell phones rather than land lines, concerns have developed about cell phone solicitations. Your cell phone should not be called by any commercial entity whom you have not given permission to contact you on that device. You do not need to put your cell phone on the FTC Do-Not-Call Registry to prevent unwanted solicitations. If you receive solicitations from organizations to which you have not given permission, notify the Federal Trade Commission. Refer to page 21 for this information.

REMOVING YOUR NUMBER FROM THE PHONE DIRECTORY

You can remove your name from the phone directory by getting an unlisted or unpublished number. Unlisted telephone numbers are not listed in a telephone directory but may be provided to electronic directory assistance (411). Unpublished telephone numbers are not publicly available (not published in a telephone directory and not available through electronic directory assistance). The most effective way to accomplish this is to get a new number rather than merely changing the status of your current number since your old number has likely been distributed to organizations and posted on the Internet. If you keep your old number, it may take 18 months or longer to have it removed from circulation. Contact your local telephone provider for more information.

OTHER OPTIONS

If you wish to remain listed in the phone book and have not placed your number on the FTC Do-Not-Call Registry, you still have several options.

COMPANY "DO-NOT-CALL" LIST

When you receive an unwanted telemarketing call, request that your personal information be placed on the company's do-not-call list. Reputable companies should honor this request.

Federal law requires that companies must honor this request if you do not have a business relationship with them. Complaints about companies that fail to honor this request should be directed to the Federal Trade Commission. The FTC website and toll-free number are provided on page 21.

As a condition of membership, the Direct Marketing Association also requires its members to offer a "Do-Not-Call" service even when you do have a relationship with them. Complaints about companies that fail to honor this request should be directed to the Direct Marketing Association. The website and phone number are provided on page 21.

LOCAL PHONE COMPANY SERVICES

Your local phone company may also offer blocking features or other technology to help prevent or screen unwanted calls. Contact them for more information about what is available in your area.

HOW CAN I PREVENT JUNK MAIL?

OPTING OUT

If you want to eliminate some of the unwanted mail and catalogs you are receiving, you can remove your name by contacting either the company sending you the mail or the list provider who supplied your name to the company. This practice is known as "opting out" and it is the most effective way to reduce the number of unwanted offers while still enjoying the mail and catalogs that are of interest to you. As a condition of membership, the Direct Marketing Association requires its members to offer a "Do-Not-Mail" service, regardless of whether you do or do not have a relationship with them. Complaints about companies that fail to honor this request should be directed to the Direct Marketing Association. The website and phone number are provided on page 23.

DIRECT MARKETING ASSOCIATION SERVICES

The DMA publishes a set of guidelines that requires its members to:

- Explain information collection and exchange practices to consumers
- Provide an opportunity for consumers to opt out of receiving promotional materials from members
- Offer consumers a way to opt out of having their name provided to other businesses for direct marketing purposes

DIRECT MARKETING ASSOCIATION COMMITMENT TO CONSUMER CHOICE

If you want to stop unsolicited direct mail from companies that you do not wish to hear from, the Direct Marketing Association offers a Commitment to Consumer Choice program to which all its members subscribe. This service allows you to specify specific companies from which you do not wish to receive direct mail, or to opt-out from all member companies. To register your preferences, go to the DMA website which is listed on page 23. The registration is good for five years. After that time, you will need to re-register. You should know that some marketers are not members of the DMA and are not bound by DMA regulations, so you may still receive unsolicited emails from these marketers.

CREDIT CARD OFFER OPT-OUT

You may receive two kinds of credit card offers. One is an invitation to apply for a card. These offers require you to fill out an application and submit it to the issuer. The other kind of offer is a pre-approved offer in which the issuer has already checked your credit history and pre-determined the credit limit for the card. The three major credit bureaus offer a toll-free number to call to opt out of receiving pre-approved offers of credit. The website and toll-free number for each of the bureaus are provided on page 23.

HOW CAN I STOP EMAIL "SPAM"?

Consumers have a number of options to prevent unsolicited email—also known as "spam." Your Internet Service Provider offers an increasingly sophisticated set of options to screen email from your inbox. Contact your service provider to understand the spam filters and personal inbox options they offer.

Legitimate businesses that collect email addresses notify you and give you the chance to "opt out" before renting or exchanging your email address with other third parties. Some offer you the chance to "opt in" by providing affirmative consent. It's always wise when you visit a website to review the company's privacy policy so you will fully understand how the information you provide will be used.

DIRECT MARKETING ASSOCIATION COMMITMENT TO CONSUMER CHOICE

If you want to stop unsolicited email from companies which you do not wish to hear from, the Direct Marketing Association offers their Commitment to Consumer Choice program to which all its members subscribe. This service allows you to specify specific companies from whom you do not wish to receive email or to opt out from all member companies. To register your preferences, go to the DMA website which is listed on page 23. The registration is good for five years. After that time, you will need to re-register. You should know that some marketers are not members of the DMA and are not bound by the DMA regulations, so you may still receive unsolicited direct mail from these marketers.

CAN SPAM ACT

In 2003 the federal government passed a law known as the CAN SPAM Act. This law requires that any email which is considered a solicitation must offer an easy way to opt out from receiving any future email solicitations from the company. If an organization fails to honor this request, contact the Federal Trade Commission at the website and toll-free number provided on page 22.

CAN I STOP COMPANIES I DO BUSINESS WITH FROM SOLICITING ME?

Absolutely. Contact these companies directly and ask them to remove your name from their marketing promotion lists. If you receive multiple mailings from the same company, you should attach a copy of each mailing label (showing any variations in your name and address) so the company can more effectively cancel all solicitations.

Most companies are quick to respond to such requests. After all, they do not want to incur the extra expense of marketing to people who do not wish to hear from them.

Be aware, however, that if you place an order later with this company through the mail, the Internet or over the phone, your name may be added back to their customer list. If this happens, you may have to repeat your request to be taken off the list. Most mail order companies and websites offer an opt out opportunity at the time an order is placed.

As described above, this service is required of all companies that are members of the Direct Marketing Association. The website and phone number are provided on page 22.

CAN I STOP COMPANIES FROM TRACKING MY ACTIVITIES ONLINE?

There are several ways you can block your online activities, which sites you visit and keywords you use to search from being recorded and used for advertising purposes. The privacy policies of the sites you visit should inform you if your visit is being recorded or if you are receiving advertisements based on your browsing on other sites and about the options you have to stop such activities.

Search engines offer the ability to opt out of the collection of information related to your searches. However, be aware that if you opt out, you may not receive certain benefits such as more relevant results from future searches.

The use of this kind of data by third parties for advertising purposes can be blocked in several ways. First, you can set your browser to either block or notify you when a third party cookie is placed on your browser. This allows you to decide when the recording begins whether you are comfortable with it or not. Second, you can go to the Network Advertiser's Initiative site

to opt out from such practices from all participating members. Contact information can be found on page 24. You may also be able to opt out at certain sites which is explained in the site's privacy policy.

Finally, you can periodically delete cookies that are placed on your browser. When you opt out, the most common practice is to put an opt out cookie on your browser which blocks future collection of information and delivery of targeted advertising. Be aware that if you delete cookies on your browser you should be careful to not delete the opt out cookies as this cancels the opt out functionality and allows collection to take place until you opt out again.

HOW CAN I CONTROL MY PUBLICLY AVAILABLE INFORMATION?

In some, but not all, instances, there are ways you can control the use of public information about you. In some cases, your options are pre-determined by state or federal law, regulations or policies. To understand your options, it is best to examine it on a case-by-case basis:

TELEPHONE DIRECTORIES

As noted earlier, phone books are considered publicly available information and are used extensively in marketing and risk applications. However, you can remove your name from the directory as described in the previous section.

REAL PROPERTY RECORDER INFORMATION

Whenever property is sold, the deed is recorded in the local county clerk's office. This record is considered a public record and is available to anyone by request. Some states and counties restrict certain types of property information. If you would like to have your name removed from public real estate records, one possible alternative is to place your property in a blind trust. For more information, contact your local county clerk's office.

OTHER PUBLICLY AVAILABLE INFORMATION

Some other public and publicly available information is contained in professional directories, drivers license information, voter registration records, hunting license records, concealed weapons permits, court records, divorce records and arrest records. Various federal and state laws, as well as industry practices, regulate the use of some or all of this information. Check with your local authorities to learn more about restrictions on the use of this information.

WHERE CAN I LEARN MORE?

There are a variety of valuable sources offering advice or publications about how information is used, what choices you have and how to protect yourself from identity fraud, including:

FEDERAL TRADE COMMISSION (FTC) CONSUMER RESPONSE CENTER

600 Pennsylvania Avenue, NW
Washington, DC 20580
Phone: Call our toll-free helpline:
877-FTC-HELP (877-382-4357)
TTY: 866-653-4261
Online: Use FTC secure complaint form
www.ftccomplaintassistant.gov/
Federal agency responsible for oversight of interstate trade and fair business practices, including the Fair Credit Reporting Act (FCRA).

FEDERAL TRADE COMMISSION'S "DO-NOT-CALL" REGISTRY

Online: Use FTC secure registration form:
www.donotcall.gov/register/reg.aspx
Phone: Call our toll-free Do-Not-Call helpline: 888-382-1222
TTY: 866-290-4236
Information on how to register for the FTC Do Not-Call registry.

FEDERAL TRADE COMMISSION'S FACTS FOR CONSUMERS

www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm
Information on how to obtain a copy of your credit report.

FEDERAL TRADE COMMISSION'S REPORT VIOLATIONS REGISTRY

Online: Use FTC secure complaint form
https://complaints.donotcall.gov/complaint/complaintcheck.aspx?panel=2
Phone: Call our toll-free Do-Not-Call helpline: 888-382-1222
TTY: 866-290-4236
If your number has been on the National Do-Not-Call Registry for at least 31 days and you receive a call from a telemarketer that should be covered by the Do-Not-Call provisions of the Telemarketing Sales Rule, file a complaint.

The FTC will need the name or telephone number of the company that called you, and the date the company called you.

FEDERAL TRADE COMMISSION'S IDENTITY THEFT REGISTRY

Online: Use our secure complaint form.
www.ftccomplaintassistant.gov/
Phone: Call our toll-free Identity Theft helpline:
877-ID-THEFT (877-438-4338)
TTY: 866-653-4261

Mail: Write to:
Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
FTC hotline to report an incident of ID theft along with other helpful advice.

FEDERAL TRADE COMMISSION'S SPAM AND PHISHING REGISTRY

spam@uce.gov
Forward unsolicited commercial email (spam), including phishing messages, directly to the FTC at spam@uce.gov. These messages will be stored in a database law enforcement agencies use in their investigations.

FEDERAL TRADE COMMISSION'S FACTS FOR CONSUMERS

www.ftc.gov/bcp/consumer.shtm
This section of the FTC website offers practical information on a variety of consumer topics.

SOCIAL SECURITY ADMINISTRATION

Phone: 800-772-1213 (TTY 800-325-0778)
www.ssa.gov/mystatement
To ask questions or report inconsistencies on your annual Social Security Statement.

UNITED STATES POSTAL SERVICE POSTAL INSPECTORS FRAUD CENTER

https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx
To report an incident of mail fraud.

DIRECT MARKETING ASSOCIATION (DMA)

1120 Avenue of the Americas
New York, NY 10036-6700
Phone: 212-768-7277
Fax: 212-302-6714
www.dmachoice.org

Trade association for most direct marketers, providing industry guidelines to protect consumer privacy. Services include:

DMA MAIL PREFERENCE SERVICE COMMITMENT TO CONSUMER CHOICE

Direct Marketing Association
P.O. Box 643
Carmel, NY 10512
www.dmachoice.org
A national do-not-mail service which all DMA member companies and organizations use.

DMA EMAIL PREFERENCE SERVICE

www.ims-dm.com/cgi/optoutemps.php
A national do-not-email service which all DMA member companies and organizations use.

BETTER BUSINESS BUREAU UNDERSTANDING PRIVACY

www.bbbonline.org/understandingprivacy/
Here you can find tips, tools and resources to keep your information private, both online and off.

CENTER FOR DEMOCRACY AND TECHNOLOGY

www.cdt.org/privacy/guide/

CONSUMER'S UNION

www.financialprivacynow.org
You can request that the three main credit reporting agencies tag your credit file with a 90-day Fraud or Victim Alert.

MAJOR CREDIT BUREAUS AND BUREAU SERVICES

EQUIFAX

Phone: 800-685-1111
www.equifax.com

EXPERIAN

Phone: 888-397-3742
www.experian.com

TRANSUNION

Phone: 888-567-8688
www.transunion.com

ONE FREE CREDIT REPORT PER YEAR

Phone: 877-322-8228
www.annualcreditreport.com

PRE-SCREENED CREDIT OFFER OPT-OUT
Phone: 888-5-OPT-OUT (888-567-8688)
(TDD service at 877-730-4105)
www.optoutprescreen.com

NETWORK ADVERTISER'S INITIATIVE (NAI)
Phone: 207-467-3500, Option 4
www.networkadvertising.org/managing/opt_out.asp

USEFUL TERMS TO UNDERSTAND

Choice is a widely shared concept in both privacy law and industry best practices. It offers individuals choices about how personal information about them is used. Consumers have the choice to not provide requested information to a company. If information is provided, then companies typically offer individuals choices relative to the use of that information for marketing purposes by the company and by others.

Credit card fraud occurs when a credit card is lost or stolen and a criminal makes purchases with the card. By law the maximum liability a consumer has for the fraudulent purchases is $50.00 and in practice most credit card issuers offer $0.00 liability.

Direct marketing describes the practice of marketing goods or services directly to consumers. The consumer may or may not have a previous relationship with the company. Direct marketing originated through door-to-door sales, but today is most commonly done through mail ("direct mail"), telephone ("telemarketing"), online email ("unsolicited commercial email") or mobile device ("unsolicited email or text messages") sometimes colloquially referred to as "Spam".

Identity takeover occurs when a fraudster has enough information to impersonate you—changing the address on your credit accounts so you do not see fraudulent charges, opening new credit accounts in your name or withdrawing funds from your existing accounts.

Notices, often called **Privacy Policies**, contain information about an institution's privacy practices. Privacy laws throughout the world are increasingly requiring that institutions provide notices about how they collect and process personal information. Depending upon specific legal requirements, the notice may include the entire privacy policy or only specified

information from the policy. Some laws require privacy notices to be posted on a website or made available upon request; others require institutions to provide customers with the notice at the time of service or at regular intervals by mail or email. They are intended both to inform consumers and others and to guide the conduct of an institution and its employees. A notice or privacy policy may be part of a larger set of legal terms or it may stand alone.

Third parties are entities with no structural legal relationship with each other. They may contract with each other or one may provide services to the other, but one does not own the other, they are not commonly owned nor do they appear commonly owned to the public.

OUR PRIVACY COMMITMENT TO YOU

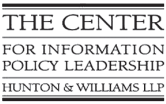
Acxiom Corporation believes that an informed consumer is a satisfied consumer. Therefore, we created this booklet to help educate you about the value received from the use of individual information and the choices you have to control its inappropriate and potentially harmful use.

We recognize that to enjoy the freedoms of our society, one must also embrace its responsibilities. For instance, the free flow of information is a cornerstone of our society and has contributed to tremendous consumer benefits and economic prosperity. Yet this freedom must be accompanied by respect for the laws and regulations that protect consumer privacy. It is this belief that has been the foundation for Acxiom as the leader in addressing consumer privacy concerns and earning the public's trust, while preserving the open system that has served the best interests of our country and its citizens for more than two centuries.

If you want to know more about Acxiom and our information practices, contact us by phone, mail or via the Internet at:

Acxiom Corporation
P.O. Box 2000
Conway, AR 72033-9928
Toll-Free: 877-774-2094
Phone: 501-342-2722
privacy@acxiom.com


Direct Marketing Association
DMA
member
Trust • Service • Value


THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP


iapp
international association of privacy professionals


iPi


CDIA
CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity


ESPC
Email Sender & Provider Coalition


MOBILE
MARKETING
ASSOCIATION


THE Information
Accountability
Foundation
COLLABORATIVE POLICY INNOVATION


iab.


Digital
Advertising
Alliance

acxiom®

Major Offices: Austin • Boston • Chicago • Little Rock • London • Munich • New York • Paris
Philadelphia • Redwood City • San Francisco • Shanghai • Singapore • Sydney • Tokyo • Warsaw

acxiom.com • privacy@acxiom.com • 888.3acxiom

AC-0262-18 1/18