To Catch a Thief:
Are Identity Theft Services Worth the Cost?

Consumer Federation of America
March 2009

To Catch a Thief: Are Identity Theft Services Worth the Cost?
Consumer Federation of America
March 2009

Table of Contents

To Catch a Thief:
Are Identity Theft Services Worth the Cost?
Consumer Federation of America
March 2009

Executive Summary

Introduction

In 2008 the Federal Trade Commission (FTC) received 313,982 complaints about identity theft, up from 258,427 complaints in 2007 and more than any other category in its Consumer Sentinel complaint database.[1] But complaints do not present the full picture; a survey conducted for the FTC found that 3.7 percent of adults in the U.S., 8.3 million people, were victims in 2005.[2] The most recent annual survey by Javelin Strategy & Research about identity fraud – the actual *use* of stolen information about individuals – showed that nearly 10 million adults were victims in 2008.[3] The rise in identity theft and fraud is probably due to several factors, including increased sophistication of the thieves, more data being collected about people, significant security breaches, worsening economic conditions, and too many consumers still being unaware of the simple precautions that they can take to protect themselves.

Stories about identity theft appear frequently in the media and surveys show that people are very concerned about the potential to become victims.[4] Capitalizing on this anxiety, many companies and organizations sell services that claim to "protect your identity." Some of these services may be helpful to consumers, but *none* can absolutely prevent their personal information from being stolen or used.

In order to find out how they claim to help consumers, Consumer Federation of America (CFA) studied the Web sites of 16 for-profit identity theft services. Generally, we found that the descriptions of the services are often confusing, unclear and ambiguous. When we attempted to call as consumers to ask for more information about how the service works, what assistance is provided to consumers who become victims, and what the

---

[1] *Consumer Sentinel Network Data Book for January-December2008,* Federal Trade Commission, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf

[2] *2006 Identity Theft Survey Report*, Federal Trade Commission, 2007, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

[3] Javelin found that the percentage of victims rose from 3.58 percent of U.S. adults in 2007 to 4.32 percent in 2008, press release February 9, 2009, http://www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-increased-22-percent-affecting-nearly-ten-million-americans-but-consumer-costs-fell-sharply-by-31-percent/

[4] For example, a survey conducted by Staples, Inc. revealed that "72 percent of Americans are more concerned about identity theft today than two years ago, 52 percent are unsure they are doing enough to protect their identities, and 43 percent wish they had more information on how to protect themselves." Press release October 9, 2007, http://investor.staples.com/phoenix.zhtml?c=96244&p=irol-newsArticle&ID=1060259&highlight=

insurance that many offer covers and excludes, we were not always able to get clear answers.

These services are not inexpensive; they generally range from $120 to $180 per year. We determined that to be of the most value, an identity theft service should have the following characteristics:

- Clearly discloses the exact services and costs.

- Monitors public and private databases and other places typically unavailable to the average consumer that may contain their personal information.

- Alerts consumers of suspicious activities related to their personal information by their choice of email, phone, text message or mail.

- Provides actual assistance, not just advice, to resolve consumers' problems if they become identity theft victims.

- Guarantees to do what it promises with no exceptions buried in fine print and no attempt to limit consumers' legal recourse through mandatory binding arbitration.

In analyzing the 16 services, it was very difficult to determine how they compared in these important criteria because the information about them was often confusing, hard to decipher, filled with hyperbole or simply missing. No company appeared to meet all the criteria.

We were most impressed by ID Watchdog and ID Theft Assist – they make clear that their main emphasis is on resolving consumers' problems if they are victims. They don't offer insurance, which is of little value, and they also offer help for pre-existing identity theft problems under certain circumstances. The Identity Theft Assistance Center also offers broad monitoring for its most expensive service and actively tries to help resolve consumers' problems (though it may not go as far in following up as the others).

There are other interesting models, but the bottom line is that none of these services is a panacea and each seems to have some shortcomings.

What Consumers Need to Know

For those consumers investigating whether or not to purchase one of these services, here are some things to consider:

- *How likely is it that you will become an identity theft victim?*
- *How much does the service cost and how does that compare with doing the same things on your own?*
- *What specific action will the service take on your behalf if you become an identity theft victim?*

Key Problems Uncovered by CFA Identity Theft Service Study

- Identity theft services often fail to provide clear, complete information about what they do and how they work.

- Some identity theft services don't disclose the cost until consumers click to enroll, making it hard to compare prices.

- Many identity theft services tout insurance as a benefit of membership, but few provide any details about exactly what the insurance covers and what restrictions or limitations apply.

- Guarantees offered by some identity theft services don't always provide the protection that consumers may expect.

- Some identity theft services make broad assurances that they will prevent consumers' personal information from being stolen or used, when none can really make that promise.

- Some identity theft services place fraud alerts preemptively on all customers' credit reports, regardless of whether they are victims or not, and make misleading claims about how the alerts will protect them.

- Many identity theft services provide customers with their credit reports as a benefit of membership. But instead of buying the reports from the credit bureaus, some services pose as their customers to request the free reports that consumers are entitled to once a year under federal law, preventing those customers from being able to get their free annual reports on their own.

- Identity theft services ask consumers to provide sensitive personal information for monitoring and other purposes, but that information could be at risk if it is not adequately safeguarded.

- Many identity theft services unfairly attempt to limit consumers' legal recourse by requiring binding arbitration for any disputes.

Policy Recommendations

Government agencies, companies and industry groups, and consumer and privacy organizations have devoted considerable effort in the last several years on improving identity theft awareness and prevention. Over the same period, dozens of for-profit identity theft services have sprung up, offering to protect and assist consumers. The time has come to turn the focus on this industry. CFA's examination of for-profit identity theft services reveals questions and concerns that should be addressed by policymakers in government and business.

- The Federal Trade Commission and state attorneys general should examine the practices of for-profit identity theft services and take enforcement action to stop abuses, including misleading advertising about the services provided and how those services protect consumers, misleading claims about the guarantees provided and how those guarantees help consumers, and practices that harm consumers' credit reports and their ability to request their free annual reports.

- The Federal Trade Commission and state attorneys general should look into whether the sensitive personal information that consumers provide to identity theft services is adequately protected from internal or external abuse. Identity theft services should be required to take adequate measures to secure customers' information and should use independent auditors to ensure that they do.

- The Federal Trade Commission should promulgate rules governing the practices of for-profit identity theft services.

- The identity theft service industry should develop best practices to encourage companies to provide clear, complete information about their services and discourage unfair or deceptive practices.

- Identity theft services should be explicitly prohibited from requesting consumers' free annual reports on their behalf.

- All consumers should have the option to place a flag on their credit reports, at no charge, that would require creditors to contact them to verify applications for new credit accounts or changes to existing credit accounts in their names.

- Consumers should have the right to check their credit reports online, whenever and however frequently they choose, at no charge.

Ten Easy Steps to Protect Your Personal Information and Detect Fraud

1. **Practice mail security.** Use a public mailbox rather than your home mailbox to send bill payments and other mail containing sensitive information. Pick your mail up promptly and ask the post office to hold it while you're away.

2. **Guard your Social Security number.** Don't carry your Social Security card, military ID, Medicare, or other cards that have your Social Security number on them unless you are going somewhere where you will need them. Only provide your Social Security number when there is a legitimate need to do so.

3. **Lock and shred.** Keep your billing and banking statements and other personal records locked up and shred them when no longer needed.

4. **Stop prescreened credit and insurance mailings.** Call toll-free 1-888-567-8688 to get off mailing lists for credit and insurance offers. Your Social Security number will be required. This keeps thieves from intercepting and accepting the offers in your name and doesn't affect your eligibility for credit or insurance.

5. **Keep private information to yourself.** Never respond to phone calls or emails asking to confirm your Social Security number or account numbers. Don't leave PIN numbers, passwords or other personal information around for others to see.

6. **Be safe online.** Use anti-virus and anti-spyware software and a firewall on your computer and keep them updated. When you provide financial or other sensitive information online, the address should change from "http" to "https" or "shttp." A symbol such as a lock that closes may also indicate that the transmission is secure.

7. **Look at your bills and bank statements promptly.** If you find any charges or debits that you never made, contact the bank or company immediately.

8. **Monitor your accounts online frequently.** You can discover problems more quickly than if you wait for bills or statements to come by mail.

9. **Check your credit reports regularly.** You can get them free once every 12 months. Go to www.annualcreditreport.com, call 1-877-322-8228, or mail your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Your name, address, Social Security number, and date of birth will be required. You don't have to get your reports from all the consumer reporting agencies at once; you can stagger your requests throughout the year.

10. **Pay attention to debt collectors.** Calls or letters about overdue accounts you don't recognize could indicate identity theft. If you are contacted by the creditor, ask for documentation about the debt; if by a collection agency, explain that you dispute the bill and why (put it in writing to maintain your debt collection rights under federal law) and ask how to contact the creditor so you can investigate.

Six Questions to Ask When Shopping for Identity Theft Services

1. **Does it monitor more than credit reports?** Since it's easy to check your own credit report and you can access it once a year for free, and because many types of identity theft don't show up in credit reports, credit monitoring alone is of limited value. Consider services that scan other commercial databases, public records, rogue Web sites that sell stolen credit cards and Social Security numbers, and other places that may have your personal information and that aren't as easy for you to monitor yourself. Also check the options for receiving alerts; some services only send alerts by email, others offer more alternatives.

2. **How does the service help if you are a victim?** Most identity theft services only provide advice about the steps you'll need to take, but some take a more active role to help resolve your problems. Depending on the terms of service, assistance may be limited to identity theft that occurs, or is discovered, after you join. If it's unclear how the service will help you, continue to shop around.

3. **Will it prevent you from getting your free annual reports when you wish?** Credit reports are often provided to customers as part of identity theft services. But some companies obtain them by requesting the free reports that you are entitled to get once a year, effectively preventing you from exercising your right to ask for your free annual report when you want it.

4. **Should you look for identity theft services that offer insurance?** Insurance generally reimburses for lost wages if you must take time off from work without pay to resolve an identity theft problem, long-distance calls, postage, notary fees and other miscellaneous expenses. Money that an identity thief has stolen from you is usually *not* covered. Since most identity theft victims have little or no expenses, insurance is not an important factor in deciding which service to buy.

5. **Does the guarantee really protect you?** No identity theft service can guarantee that you won't become an identity theft victim. Guarantees are promises about what the service will do if you are victimized. They may provide for expense reimbursement and/or assistance resolving your problem. Some only promise to resolve problems resulting from a defect in the service. Read the guarantee carefully; it may not provide as much protection as you expect.

6. **What are the costs and terms?** Many identity theft services offer "free trials," during which you can test some of the features, but unless you have an identity theft problem immediately, you can't fully assess the service during the trial period. Pay attention to the terms of the trial offer; usually consumers must cancel before it ends to avoid charges. Some services charge month-to-month, others require payment upfront for a year or offer pre-payment options that are less expensive than paying month-to-month. Not all will provide a pro-rated refund if you decide to cancel before the term you paid for is up, however. Read the terms and conditions carefully to understand the cancellation policy.

Background on CFA's Identity Theft Service Study

This study was undertaken with support from the Rose Foundation for Communities & the Environment Consumer Privacy Rights Fund. The objective was to help individuals understand their legal rights and options to protect their identities, decide whether to purchase identity theft services, and know what to look for and what to avoid in shopping for these services. Another important aspect of the study was to identify problems with fee-based identity theft services and recommend policy measures to address them.

CFA's aim was to look at identity theft services from the consumer's perspective and ask the following questions:

- What types of identity theft services are offered in the marketplace? How are the services described?
- What do they cost?
- Do they provide the information that consumers need to make comparisons and decide whether to purchase these services and which ones might serve them best?
- Are any of the claims they make inaccurate or misleading?
- What are the benefits of using the services? Are there any downsides?
- How do the services provided compare to what consumers can do to protect themselves?

Between September 2008 and February 2009 CFA staff examined the Web sites of a variety of identity theft services and, when necessary, contacted customer service at the phone numbers or email addresses provided to ask questions. We also looked for lawsuits and other publicly available information concerning the services. CFA did not actually purchase or test any of the services, and this study does not attempt to rate their effectiveness.

To Catch a Thief: Are Identity Theft Services Worth the Cost?

Consumer Federation of America
March 2009

The Scope and Impact of Identity Theft

What is identity theft?

The Identity Theft and Assumption Act of 1998 made it a federal crime when anyone "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."[5] Simply put, identity theft is obtaining, possessing, sharing or using something that can identify another person, such as a Social Security number, driver's license number, financial account number, or biometric data, without any legal right and with the intent to something illegal with it.

Identity theft runs the gamut from one family member stealing another's Social Security number to fraudulently apply for a loan to organized gangs selling stolen credit card numbers on the Internet. But it's not just about credit. Stolen personal information can be used to get a job, medical treatment, utility services, or housing; to hide one's true identity in order to evade responsibility for a crime or a debt; to steal money from people's financial accounts; and to obtain government benefits or documents.

Some argue that the term "identity theft" should only be used when someone creates a *new* account with stolen information, not when an imposter uses an *existing* account belonging to another person. However, the federal statute is very broad, and identity theft statistics usually encompass both new accounts and account-takeovers.

How big is the problem?

In 2008 the Federal Trade Commission (FTC) received 313,982 complaints about identity theft, up from 258,427 complaints in 2007 and more than any other category in its Consumer Sentinel complaint database.[6] But complaints do not present the full picture; a survey conducted for the FTC found that 3.7 percent of adults in the U.S., 8.3 million people, were victims in 2005.[7] The most recent annual survey by Javelin Strategy & Research about identity fraud – the actual *use* of stolen information about individuals –

---

[5] Public Law 105-318, 18 U.S.C. 1028 (a) (7)
[6] *Consumer Sentinel Network Data Book for January-December2008,* Federal Trade Commission, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2008.pdf
[7] *2006 Identity Theft Survey Report*, Federal Trade Commission, 2007, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf

showed that nearly 10 million adults were victims in 2008.[8] The rise in identity theft and fraud is probably due to several factors, including increased sophistication of the thieves, more data being collected about people, significant security breaches, worsening economic conditions, and too many consumers still not taking the simple precautions necessary to protect themselves.

Stories about identity theft appear frequently in the media and surveys show that people are very concerned about the potential to become victims.[9] Capitalizing on this anxiety, many companies and organizations sell services that claim to "protect your identity." Some of these services may be helpful to consumers, but *none* can absolutely prevent their personal information from being stolen or used.

What is the impact of identity theft on victims?

It is unnerving to discover that your personal information has been stolen, whether it has been used by someone else or not. Resolving problems if it has been used can cost time and money. According to the Identity Theft Resource Center (ITRC), a nonprofit organization that provides advice and education, victims who responded to its 2007 survey[10] spent an average of 116 hours and $550 to repair the damage that identity thieves caused to existing accounts and even more time and money when the thieves created new accounts. Expenses included postage, copying, obtaining police reports and court records, travel, attorneys' fees, and childcare. Seventy percent of victims said that it took up to a year to clear all the misinformation from their records, and not all succeeded. Victims also reported that the identity theft sometimes had secondary effects, such as increasing their credit card interest rates or causing stress in the family.

In the FTC survey, many of the victims experienced more than one type of identity theft.

- The most common was misuse of an existing credit card account, a problem encountered by 58.9 percent of the victims; *for 38.1 percent of victims that was the only problem they had*. Fortunately, for reasons we describe later in this report, that is the easiest type of identity theft for consumers to resolve.

- The next most common category of identity theft, experienced by 48.6 percent of the victims, was misuse of existing non-credit card accounts such as utility

[8] Javelin found that the percentage of victims rose from 3.58 percent of U.S. adults in 2007 to 4.32 percent in 2008, press release February 9, 2009, http://www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-increased-22-percent-affecting-nearly-ten-million-americans-but-consumer-costs-fell-sharply-by-31-percent/

[9] For example, a survey conducted by Staples, Inc. revealed that "72 percent of Americans are more concerned about identity theft today than two years ago, 52 percent are unsure they are doing enough to protect their identities, and 43 percent wish they had more information on how to protect themselves." Press release October 9, 2007, http://investor.staples.com/phoenix.zhtml?c=96244&p=irol-newsArticle&ID=1060259&highlight=

[10] *Identity Theft: The Aftermath 2007*, Identity Theft Resource Center, http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2007_20080529v2_1.pdf

accounts, checking and savings accounts, Internet payment accounts, email and Internet accounts, and medical insurance.

- Less than a quarter of victims, 22 percent, suffered from new accounts being opened or other frauds being committed using their personal information.[11] That included five percent who said that an identity thief had given their names to the police when stopped or charged with a crime.[12]

Nearly 40 percent of victims discovered the problems in less than a week, but it took longer for victims of new accounts and other frauds to discover the problems[13] and to resolve them[14] than it did those whose existing accounts had been compromised. Generally, the earlier victims discovered the problems, the lower their out-of-pocket expenses.[15] The average amount of out-of-pocket expense was $377[16] and the majority of victims had no out-of pocket expenses.[17] In the FTC's survey report, out-of-pocket expenses include costs to resolve the problems, such as notary fees, postage, lost wages and legal fees *and* payments for any fraudulent debts incurred by identity thieves. There is no information about how much of the out-of-pocket expenses were for payment of fraudulent debts. *As we will explain later, victims are generally not responsible for debts incurred by identity thieves.*

The median (the point at which half the victims fell above the number and half below) amount of time spent resolving the problems was 4 hours.[18] (The ITRC figures may be higher than the FTC's because they are based on victims who contacted that organization for help and whose situations might have been more severe than those of randomly surveyed identity theft victims.)

The Javelin survey showed that while the number of victims increased from 2007 to 2008, the out-of-pocket expenses they incurred decreased from an average of $691 to $496.[19]

Given the disparate survey data, it's difficult to assess exactly how much identity theft costs victims. *Some victims may need to spend significant amounts time and money to resolve their problems, but most do not.*

---

[11] *2006 Identity Theft Survey Report*, Federal Trade Commission, 2007, http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf at 13
[12] Id at 21
[13] Id at 23
[14] Id at 25 and 26
[15] Id at 24
[16] Id at page 9
[17] Id at page 37
[18] Id at page 39
[19] *2009 Identity Fraud Survey Report*, Javelin Strategy & Research, press release February 9, 2009, http://www.javelinstrategy.com/2009/02/09/latest-javelin-research-shows-identity-fraud-increased-22-percent-affecting-nearly-ten-million-americans-but-consumer-costs-fell-sharply-by-31-percent/

Resources to Help Consumers Deal with Identity Theft

Personal information can be stolen many ways, from low-tech methods such as rummaging through mailboxes and dumpsters, to computer hacking and other high-tech tactics. It is difficult to assess one's vulnerability to identity theft; in the FTC and Javelin surveys, the majority of victims had no idea how their information was stolen. However, there are many steps consumers can take themselves, at little or no cost, to reduce their potential to become identity theft victims and detect fraud (see Appendix A).

Despite the claims that some make, no identity theft service can absolutely prevent one's personal information from being stolen or used.

How helpful are credit monitoring services?

Credit monitoring services alert consumers when there are activities in their credit bureau files that might indicate identity theft, such as new credit applications, new credit accounts opened in their names, requests to change the billing address, increases in their credit limits, and negative information such as overdue payments. Alerts are usually provided by email, though some services offer additional alert options.

The value of credit monitoring is limited by its narrow scope. Many types of identity theft, such as those involving account takeovers, employment, utility accounts, medical services, and government benefits, may not show up in credit bureau files. Furthermore, since consumers can check their files themselves for free once a year, and more frequently, if they desire, at relatively low cost (or at no charge if they are fraud victims and in other situations as described in this report), and since those with Internet access can monitor their financial accounts online, it may not make sense to pay $10 or more per month for a credit monitoring service.

If consumers are interested in purchasing identity theft services, they should start by looking at those that offer a broader range of features than just credit monitoring.

What other types of for-profit identity theft services are there?

CFA found a wide range of for-profit identity theft services that go beyond just credit monitoring. Some services monitor customers' personal information more widely (in addition to or instead of monitoring credit reports), searching various commercial and public databases, online chat rooms, and "underground" Web sites that identity thieves use to trade in stolen credit card numbers, bank account numbers, Social Security numbers, and other information. Other services operate primarily by placing fraud alerts on consumers' credit files.

Most services offer some type of assistance for customers who become identity theft victims, from providing advice to taking direct action to resolve their problems. For some services, fraud resolution is the main benefit they provide. Many services include insurance or guarantees.

What do identity theft services cost?

The cost of the 16 identity theft services we examined varied from $24 per year for a very narrowly tailored service to $359.40 per year, but most of them were in the $120 to $180 range. Some services charge monthly fees, others offer subscriptions for a year or longer, and some provide both options. When comparing the cost of identity theft services, consumers should multiply monthly charges by 12 to get the annual cost (we provide that information in this report).

What free or low-cost options are there for consumers?

As we explain in more detail later in this report, consumer can request their credit reports free once a year and the maximum charge to buy them is currently $11 (see Appendix C for tips on how to detect financial fraud). Placing a freeze on one's credit file generally costs $5 to $10; in some cases it may be free. It costs nothing for identity theft victims to place fraud alerts or get their credit reports.

Identity theft victims can get advice free from many sources, including:

- The Federal Trade Commission, http://www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-ID-Theft (1-877-438-4338), TTY 1-866-653-4261, provides comprehensive advice in both English and Spanish about the steps that identity theft victims should take and the affidavits, forms and sample letters they need.

- The Privacy Rights Clearinghouse offers advice for identity theft victims through fact sheets and other materials at http://www.privacyrights.org/identity.htm.

- The Identity Theft Resource Center provides advice for victims on its Web site, http://www.idtheftcenter.org/, and offers personal counseling for those who need more guidance at 1-858-693-7935 or victims@itrc.org (note that this is a toll call, operating hours are Monday-Friday, 9 a.m. to 4:30 p.m. Pacific standard time).

- Call For Action has trained volunteers that will walk victims through the steps needed to resolve their problems and provide follow up support until they are resolved, www.callforaction.org, 1-866-ID-HOTLINE.

In addition to providing advice, the FTC takes complaints about identity theft in order to track trends, and in some cases passes the information along to private entities when it believes that sharing information might help resolve identity theft-related problems. However, the FTC does not attempt to resolve individuals' identity theft problems. All complaints are entered into the FTC's database, which is accessible to federal, state and local law enforcement agencies. By aggregating complaint information, the FTC and other agencies can identify situations that may merit investigation and legal action – for instance, those involving large numbers of victims.

Another benefit of filing identity theft complaints with the FTC is that victims can print their completed complaint forms as the official "identity theft reports" that are required to exercise certain rights under the Fair Credit Reporting Act.[20] Victims are encouraged to report identity theft to their local police, even though they may unwilling or unable to help, in order to have a police report on file in case it's needed.

Identity theft victims can also contact their state offices of attorneys general and other state and local consumer protection agencies for advice. They are listed in the state and local government sections of the telephone book (for a list of state offices of attorneys general go to http://www.naag.org/attorneys_general.php). In some cases, these agencies may take complaints and attempt to help victims resolve their problems.

Nonprofit consumer organizations are another good resource for identity theft victims. Consumer Action, for example, offers educational brochures and training materials about identity theft to individuals and community groups at no charge.[21]

The credit bureaus provide information on their Web sites about how to deal with identity theft.[22] Many banks and other financial service companies also offer advice on their Web sites, and some even provide free assistance to customers who are identity theft victims.[23] In addition, when companies, agencies or organizations experience security breaches, they often offer to pay to provide identity theft services to affected consumers.

Consumers may be unaware of another free resource, the Identity Theft Assistance Center (ITAC). This nonprofit organization, supported by many major banks and other financial service companies, helps identity theft victims by providing counseling and relaying information about their problems to law enforcement agencies, consumer reporting agencies, creditors, and others as needed.

To get free assistance, consumers must be referred to ITAC by a member company with which they have an account (see http://www.identitytheftassistance.org/ for the list of ITAC member companies). The identity theft does not need to be related to that account in order to be referred. ITAC requires member companies to respond to consumers within two days of being notified of their problems. However, ITAC may not be able to resolve all consumers' problems, especially if companies that are not members of ITAC fail to respond. ITAC also sells identity theft services, which are described later in this report.

Why buy identity theft services?

Most consumers will probably never be identity theft victims, and the most common problem, fraudulent charges on an existing credit card, is easy for consumers to resolve

[20] 15 U.S.C. 1681 et seq.
[21] See http://www.consumer-action.org/english/library/C36
[22] For example, see advice at http://www.experian.com/identity_fraud/fraud_prevention.html on the Experian Web site.
[23] For example, Citibank provides information, and free assistance for customers, see https://web.da-us.citibank.com/cgi-bin/citifi/portal/ps/detail.do?BV_UseBVCookie=yes&BS_Id=IDTheft

themselves. Furthermore, there are many things that consumers can do themselves to reduce the potential for identity theft and sources for free help if they are victimized.

Some identity theft services can help consumers detect some types of identity theft more quickly than they could on their own by alerting them to fraudulent credit applications, checking databases to which consumers may not have easy access, and detecting if their information is for sale in "underground" Web sites, chat rooms, and other places on the Internet where stolen personal information is traded. The assistances provided that some services provide to victims may also be helpful if they go beyond advice to actively help resolve their problems.
For those consumers investigating whether or not to purchase one of these services, here are some things to consider

- *How likely is it that you will become an identity theft victim?*
- *How much does the service cost and how does that compare with doing the same things on your own?*
- *What specific action will the service take on your behalf if you become an identity theft victim?*

Six key questions to ask about identity theft services are provided in Appendix B.

What characteristics provide the best value?

We determined that to be of the most value, an identity theft service should have the following characteristics:

- Clearly discloses the exact services and costs.

- Monitors public and private databases and other places typically unavailable to the average consumer that may contain their personal information.

- Alerts consumers of suspicious activities related to their personal information by their choice of email, phone, text message or mail.

- Provides actual assistance, not just advice, to resolve consumers' problems if they become identity theft victims.

- Guarantees to do what it promises with no exceptions buried in fine print and no attempt to limit consumers' legal recourse through mandatory binding arbitration.

In analyzing the 16 services, it was very difficult to determine how they compared in these important criteria because the information about them was often confusing, hard to decipher, filled with hyperbole or simply missing. No company appeared to meet all the criteria.

We were most impressed by ID Watchdog and ID Theft Assist – they make clear that their main emphasis is on resolving consumers' problems if they are victims. They don't offer insurance, which is of little value, and they also offer help for pre-existing identity theft problems under certain circumstances. The Identity Theft Assistance Center offers broad monitoring for its most expensive service and actively tries to help resolve consumers' problems (though it may not go as far in following up as the others).

There are other interesting models, but the bottom line is that none of these services is a panacea and each seems to have some shortcomings.

Consumers' Rights Related to Identity Theft

What are consumers' rights concerning the security of their personal information?

It is difficult for consumers to control the security of their personal information completely because in many cases it's out of their hands. Doctors, lawyers, banks, brokerages, schools, government agencies, retailers, charities, commercial data brokers, and many others collect and store people's personal information, and the potential for internal or external theft hinges on their security practices. According to Privacy Rights Clearinghouse, a nonprofit consumer and privacy advocacy organization, more than 252 million data records of U.S. residents have been exposed due to security breaches since 2005.[24] Those are only data breaches that have been publicly reported; no one knows the total number or how many people's information has been fraudulently used as a result.

While there is no federal law requiring that individuals be notified about security breaches, most states have enacted such laws.[25] Who is covered and under what circumstances breach notifications must be sent varies. Often, consumers don't discover that their identities have been stolen until they find unauthorized charges or debits on their statements or someone contacts them about an unpaid bill. If their identities have been used for criminal activities or employment, they may not be aware until police or IRS agents knock at their doors.

Some federal laws specifically require securing personal information. For example, under the Gramm-Leach-Bliley Act, "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[26] Doctors, health plans and others covered by the Health Information Portability and Accountability Act of 1996 (HIPAA)[27] must ensure the "confidentiality, integrity, and availability" of electronic health records.[28]

---

[24] See chronology of breaches at http://www.privacyrights.org/ar/ChronDataBreaches.htm, last accessed 2/5/09

[25] Consumers Union tracks state security breach laws, see http://www.consumersunion.org/campaigns//financialprivacynow/002215indiv.html

[26] 15 U.S.C. 6801 § 501

[27] Public Law 104-191

[28] 45 CFR 164.306

However, there is no federal law that requires information security broadly across all sectors, and where there are security requirements as in the examples above, individuals often lack the right to sue to enforce them.

Most legal rights and responsibilities related to identity theft are aimed at preventing the *use* of stolen personal information and minimizing the potential damage. For instance, under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act)[29] the Federal Trade Commission (FTC) and the federal bank regulatory agencies have issued new regulations called the Red Flag Rules,[30] which require financial institutions and creditors to develop written plans to identify and respond to warning signs of identity theft, such as unusual activity on an account, address discrepancies, or use of suspicious application documents (the effective date has been delayed from November 1, 2008 to May 1, 2009).

Is consumers' personal information required to be encrypted?

Encryption turns information into code that can only be read by those who have the key to decode it. When consumers make purchases online and the address bar changes from "http" to "https" or "shttp," that's an indication that encryption is being used to protect their financial information as it is being transmitted to the company. Encryption can also be used to keep personal information safe when it is stored in databases and on laptop computers or transmitted from one company to another. There is no federal requirement for businesses, organizations or government agencies to encrypt people's personal information, but some states are starting to enact encryption requirements.[31]

What are consumers' rights concerning credit reports?

The FCRA governs "consumer reporting agencies" that compile and sell information about individuals for "permissible purposes" such as to establish their eligibility for credit, insurance and employment. Information in consumers' files may also be used to determine the rates they pay for credit or insurance, their credit limits, their eligibility for professional licenses, how much they should pay for child support, and other purposes.

Of the many rights that individuals have under the FCRA, this report will focus on those that are particularly relevant to preventing the use of stolen personal information and remedying the problem if someone is a victim.[32]

Many identity theft services offer to do things that consumers have the right to do themselves for free or at minimal cost.

---

[29] Public Law 108-159

[30] See http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf

[31] For instance, see Massachusetts regulations, 201 CMR 17.00 http://www.mass.gov/?pageID=ocaterminal&L=3&L0=Home&L1=Consumer&L2=Identity+Theft&sid=Eoca&b=terminalcontent&f=idtheft_201cmr17&csid=Eoca

[32] For more details about credit report rights under FCRA, see the two FTC fact sheets, *A Summary of Your Rights Under the Fair Credit Reporting Act*, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre35.pdf, and *Remedying the Effects of Identity Theft*, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt09.pdf

The files at consumer reporting agencies generally contain four types of information:

- **Personal information** such as name, address, employer and social security number;
- **Credit information** listing accounts, balances and credit limits, and timeliness of payments;
- **Public records** such as bankruptcies, tax liens, judgments, child support orders, and arrests;
- **Inquiries** which show who has obtained the file and when.

Most of the information in consumers' files is provided by the banks, retailers, and other companies with which consumers have direct relationships. Equifax, Experian, and TransUnion are the three major consumer reporting agencies that operate nationwide. Since much of the information they collect is about consumers' credit histories and one of the main uses of that information is to make decisions about consumers' credit worthiness, these consumer reporting agencies are often referred to as credit bureaus and the reports they provide as credit reports. When consumer reporting agencies provide consumers with their reports, these are sometimes called "consumer disclosures."

There are also "specialty agencies" such as the Medical Information Bureau, a database of information about payment of medical bills,[33] and ChexSystems, which collects information about consumers who have mishandled their checking or savings accounts.[34] Some creditors and employers don't provide data to any consumer reporting agencies, and some provide information to certain ones but not others, so the information that is available about an individual may vary from one company's files to another. Public records in a consumer's file may vary, too, since many courts, deed registries and other government offices are not equipped to provide them in an easily accessible form. Some types of public records, such as drivers' licenses, are not collected by consumer reporting agencies at all.

What are consumers' rights to see their information?

Consumers have the right to see the information about them in files that are covered by the FCRA. They can purchase their reports whenever they want. The FTC limits the fee that consumer reporting agencies can charge consumers for their reports and adjusts it annually for inflation. For 2009 the maximum fee is set at $11.00. Credit bureaus also offer a bevy of other products for sale, including "3-in-1" reports that combine information from all three, which can sometimes be more economical than buying reports separately from each one, and packages that include credit scores (consumers have the right to buy credit scores separately if they choose).

[33] See information about specialty reporting agencies from Privacy Rights Clearinghouse at http://www.privacyrights.org/fs/fs6b-SpecReports.htm

[34] See information about ChexSystems at https://www.consumerdebit.com/consumerinfo/us/en/index.htm

CFA found information about purchasing the basic credit report easily on Experian's Web site, but it was difficult to find on the Equifax Web site and we couldn't find it at all on TransUnion's site.

However, for most people who simply want to check their credit reports once a year it's not necessary to buy them because they have the right under the FCRA to request one *free* report every 12 months from *each* of the consumer reporting agencies that operate nationwide. There is a special Web site, toll-free number, and mailing address for consumers to use to request their free annual credit reports.[35] In addition, some states give residents the right to request free reports annually.[36] Consumers' rights to request free reports under state law are in *addition* to their rights to free reports under federal law.

Experts recommend that consumers stagger requests for their free credit reports throughout the year rather than getting them from all at the same time.

Consumers should be wary of advertisements for "free credit reports." These have nothing to do with the free annual reports that consumers are entitled to request under federal law – they are solicitations from companies that sell credit monitoring and other services. In 2005 the FTC settled a lawsuit against Consumerinfo.com, doing business as Experian Consumer Direct, for failing to adequately disclose to consumers who responded to its ads for free credit reports that they would be automatically enrolled in a credit report monitoring service and charged $79.95 unless they cancelled within 30 days. The company agreed to disclose the terms of its offers more clearly.[37] However, concerns remain that offers for "free credit reports" can be misleading.

The FCRA also entitles consumers to request free copies of their reports directly from consumer reporting agencies if they are:

- Denied credit, insurance, or employment on the basis of information in a report (the request goes to the one that provided the report); unemployed and planning to look for a job within the next 60 days;

- On welfare (the limit is one from each consumer reporting agency per year); or

- Suspect that they are a victim of fraud, including identity theft (more details about this are provided later).

Requesting reports under these circumstances does *not* affect an individual's ability to obtain the free annual reports.

---

[35] For details see *Facts for Consumers, Your Access to Free Credit Reports*, FTC, http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre34.shtm

[36] See Frequently Asked Questions, AnnualCreditReport.com, https://www.annualcreditreport.com/cra/index.jsp

[37] See FTC warning at http://www.ftc.gov/freereports

What are security freezes?

A security freeze prevents identity thieves from using stolen personal information by "locking" the consumer's file so no one can get access to it (except for creditors with whom the consumer already has an account and government agencies in certain situations). Security freezes are mainly useful for blocking fraudulent attempts to open new accounts using a consumer's stolen information (however, not all companies bother to check consumers' reports when applications for new accounts are made). Consumers can use PIN numbers to lift the freeze if they are planning to do something that requires a credit check and to "refreeze" their files. A security freeze lasts until the consumer removes it. To place a security freeze at each consumer reporting agency, the individual must contact them separately.

There is no federal security freeze law, but most states have enacted security freeze laws. They vary in terms of who can request a freeze (only victims or anyone) and the amount that can be charged, if anything, for placing and lifting freezes. Consumers who live in states without security freeze laws or whose laws only provide for freezes for identity theft victims can request freezes the consumer reporting agencies under a voluntary program for a small fee.[38] The process and timeline for setting and lifting freezes varies with each.

Security freezes can help deter certain types of credit-related identity theft but they don't provide blanket protection from one's stolen information being used.

What are consumers' rights to remedy problems in their reports?

In some cases consumers only learn that they are identity theft victims when they are denied credit or employment based on negative information in their files caused by imposters. Consumers should check their credit reports at least once a year, and even more frequently if they are planning to apply for a mortgage or a new job, or if they have been victims of identity theft in the past, because spotting problems and resolving them quickly helps to avoid bigger problems later. The FCRA gives consumers the right to dispute any information in their files that they believe is inaccurate or incomplete, at no charge.

Once the consumer reporting agency is notified about the disputed information, it must investigate within 30 days. It does so by contacting the source of the information. It must also take into consideration any relevant information that the consumer provides. If the disputed information is found to be incomplete or inaccurate, or can't be verified, the consumer reporting agency must correct or delete it as appropriate.

It is not possible to remove negative information that is accurate, as bogus credit repair services offer to do. If the information is correct, it generally stays on credit reports for seven years; bankruptcies for ten.

---

[38] Consumers Union tracks state security freeze laws and provides information about the voluntarily freezes at http://www.consumersunion.org/campaigns/learn_more/003484indiv.html

Mistakes such as transposed digits or closed accounts that appear as open are relatively easy to deal with. But when people discover that identity thieves have impersonated them to borrow money, make purchases using their accounts, set up new accounts, get jobs, or for other fraudulent purposes, resolving those problems can sometimes be difficult.

To make it easier, identity theft victims have the right to:

- Demand that businesses give them copies of the applications and other documents related to the disputed transactions or accounts;

- Demand that debt collectors give them information about debts they believe were incurred by an identity thief, such as the creditors' names and amounts owed;

- Block information that they believe resulted from identity theft from appearing on their reports;

- Prevent businesses from reporting information that they believe resulted from identity theft to consumer reporting agencies.[39]

Victims must document that they have filed an "identity theft report" with a local, state or federal law enforcement agency in order to block information resulting from identity theft from appearing on their reports or prevent businesses from reporting it. This is a sworn statement of the facts to the best of the person's knowledge. A police report may or may not suffice as an identity theft report depending on whether it has adequate detail; the Federal Trade Commission provides advice in this regard.[40] There is no charge to file an identity theft report, though you may be asked to pay a fee to obtain copies. Identity theft reports can also be used to stop debt collectors from continuing to contact victims about unpaid bills that identity thieves have incurred.

What are fraud alerts?

Under the FCRA, individuals can place fraud alerts on their files. There are three types.[41] An "initial alert" can be requested by "a consumer or someone acting on behalf of or as a personal representative of a consumer who asserts in good faith a suspicion that the consumer has been or is about to become a victim of fraud or related crime, including identity theft." This language makes clear that an initial alert is intended to protect people who have reason to think they are victims or *could* be victims imminently – for instance, if they've lost their wallets or received notice of a security breach.

When creditors see an initial fraud alert in a consumer's credit report, it warns them that the person may be a victim and requires them to use "reasonable policies and procedures"

[39] For more details about victims' rights, go to the FTC's special identity theft Web site, http://www.ftc.gov/bcp/edu/microsites/idtheft/
[40] See information from the FTC about identity theft reports at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html#Whatisanidentitytheftreport
[41] 15 U.S.C. § 1681c-1

to verify the identity of anyone who is applying for credit, asking for a credit limit to be increased, or requesting an additional credit card as that person. The consumer can provide a phone number for verification purposes, but there is *no* requirement for creditors to call or contact the consumer by other means. They can take any steps they deem "reasonable" to verify the person's identity. An initial alert is meant to be short-term; it lasts for 90 days, unless the consumer asks to remove it sooner, and it can be renewed if necessary.

It is very easy to place an initial fraud alert by phone or online. The process is automated and takes just seconds to do.

An "extended alert" is for people who believe that they definitely *are* fraud victims and want extra protection. It requires an official identity theft report and stays on the credit file for 7 years unless the consumer asks for it to be removed sooner. When creditors see an extended alert, they *must* contact the consumer before granting credit, increasing the credit limit, or providing an additional credit card to someone claiming to be that person. They can do so by phone, or the consumer can designate another way to be contacted.

Neither the initial nor the extended alert is intended as a shield to protect consumers who are simply concerned that they *might* someday become fraud victims. On the other hand, the "active duty alert" *is* meant to be prophylactic because it is more difficult for military personnel serving in places such as Baghdad or Afghanistan to monitor their accounts and credit reports and detect possible identity theft than it would be if they were at home. All military personnel on active duty away from their normal duty stations are entitled to request this type of alert, even though they have no reason to suspect that they are or are about to become identity theft victims.[42] The alert stays on the file for one year unless the person asks for it to be removed sooner and can be renewed if deployment lasts longer. Creditors' duties to use "reasonable policies and procedures" are same as for initial alerts.

Consumers only need to contact one of the three major consumer reporting agencies to request a fraud alert; that agency will transmit the request to the others so the alert will show up in the files at all three. There is no charge to request a fraud alert. The consumer reporting agencies must respond to the request for alerts by notifying the consumers that they may request a free credit report (one for initial alerts and up to two within the next 12 months for extended alerts).

The main benefit of fraud alerts is that they make it harder for identity thieves to open new accounts in their victims' names, but they don't make it impossible. Not everyone who has a "permissible purpose" to get a consumer's credit report does so. The "reasonable policies and procedures" that a creditor must take if it sees an initial or active duty alert may not work – for example, the identity thief may be able to provide the correct additional information if asked – and only apply to certain situations involving credit, not to employment or other uses of credit reports. And fraud alerts don't prevent identity thieves from successfully impersonating their victims in situations where credit

[42] See FTC Consumer Alert at http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt147.shtm for more details about active duty alerts

reports would not normally be needed, such as applying for government benefits, obtaining medical treatment, using existing accounts to make purchases, getting a driver's license, withdrawing money from a bank account, or being arrested.

Fraud alerts can have negative consequences for consumers and should not be requested without good reason. When they see fraud alerts on the files, some creditors may simply the deny credit application rather than taking further steps to verify the applicant's identity before granting credit. This can result in people being denied credit who really are who they claim to be. If consumers apply for credit repeatedly because of such denials, that can harm their credit scores.

Fraud alerts and security freezes may cause some inconvenience for consumers as well as for identity thieves. Consumers may be required to provide additional identification or information for certain credit transaction, and may be unable to obtain "instant credit" at a store. Also, the process for lifting a security freeze could delay some transactions.

How can consumers stop mailings for credit cards or insurance?

When individuals request extended or active duty alerts on their files, the FCRA requires the consumer reporting agencies to remove them (for 5 years and 2 years, respectively) from the mailing lists that the agencies compile for credit card issuers and insurance companies to send consumers unsolicited offers of credit or insurance. This prevents identity thieves, who may steal their victims' mail or change the addresses on their accounts, from receiving these "prescreened" offers and accepting them in their victims' names. The FCRA provides that *any* consumer, whether a victim of identity theft or not, can get off the mailing lists for these offers by calling toll-free, 1-888-567-8688. There is no charge and the consumer can renew the opt-out every 5 years or remove it at any time.

Opting out will not stop all credit card and insurance solicitations, but it will significantly reduce them.

Are consumers' responsible for unauthorized credit or debit transactions?

Stolen personal information is most commonly used to take over existing financial accounts or create new accounts in the victims' names. Federal regulations give consumers the right to dispute unauthorized transactions on credit card or charge accounts[43] and electronic fund transfers from their bank account.[44] Consumers are liable for only $50 if they report the fraud to the financial institution or card issuer as soon as they discover it, and in most cases even that amount is waived under issuers' "zero liability" policies. The compromised account numbers are cancelled and new ones issued.

Consumers' rights if identity thieves steal their checks or take money from their bank accounts using forged withdrawal forms are covered by state law. Generally, they are not liable for losses if they report the fraud promptly. In some cases, a notarized statement,

[43] Regulation Z, see in particular 12 CFR § 226.12(b)
[44] Regulation E, see in particular 12 CFR § 2056(b)

police report, or other documentation may be required, but these types of problems are usually fairly easy for consumers to resolve.

Identity thieves sometimes use stolen personal information to obtain utility services or merchandise for which their victims will be billed. Under state contract laws, consumers are not liable for contractual agreements that they did not make.

What if consumers' personal information is used for employment fraud?

Stolen personal information is a hot commodity for illegal aliens and others whose circumstances make it difficult to get jobs using their true identities. Often, victims don't know that their identities are being used by others for employment purposes until they are contacted by the Internal Revenue Service or another government agency. Consumers are not responsible for income tax obligations incurred by identity thieves. To resolve these types of problems, they may be asked for proof of employment or other documentation.

What if consumers' personal information is used to fraudulently obtain government benefits?

Identity thieves may use stolen personal information to fraudulently obtain Social Security payments, disability benefits, or other government benefits such as driver's licenses. This could make it difficult for victims to get the benefits to which they are legitimately entitled. Victims should notify the relevant government agency as soon as they discover the problem and provide any documentation that is required.

What if consumers' personal information is fraudulently used to obtain medical services?

Of all the ways that stolen personal information may be used, medical identity theft is the most alarming. It's not just a matter of clearing up the bills for medical services that imposters have obtained using their victims' information – like other debts, identity theft victims cannot be held responsible for those charges. But their health can actually be endangered if information about other people's conditions is mixed into their medical records. HIPAA entitles consumers to access to their medical records. However, there may be a charge to do so and amending the records can be difficult.[45]

What if consumers' personal information is fraudulently used in court?

Some identity theft victims are shocked to discover that their personal information has been used by imposters in civil or criminal cases. Since the ease with which records are available from courts varies widely, this information doesn't always show up in consumers' credit reports. Unlike most identity theft problems, which victims can generally resolve on their own, untangling these situations may require hiring an attorney.

[45] The nonprofit organization World Privacy Forum has detailed information about medical identity theft and tips for how to resolve problems at http://www.worldprivacyforum.org/medicalidentitytheft.html

To help people avoid the problems that can arise when identity thieves impersonate them in criminal proceedings, California has created identity theft registry. Police can check it to verify that someone is an identity theft victim, not the person they are looking for.[46] Some states have also implemented "identity theft passport" programs that enable people to carry cards vouching for the fact that they are documented identity theft victims.[47]

Are all data brokers covered by the FCRA?

While consumer reporting agencies are regulated by the FCRA, other "data brokers" – companies that compile information about people from a variety of public and private sources and offer that information for sale – don't necessarily come under those rules. Whether or under what circumstances they do is complicated and confusing. For instance, the FCRA applies when a data broker furnishes an employer with a background check on an individual, but not if the employer simply buys information about the individual from a data broker and conducts its own background check.[48]

The number of data brokers is proliferating, especially online. Most consumers are unaware that they exist and there is no requirement for them to notify consumers that they are compiling information about them. Some will remove consumers' information from their databases voluntarily on request, others will not.[49] Other than the narrow constraints of the FCRA, federal law does not restrict data brokers to selling consumers' personal information only for "permissible purposes" or require them to give consumers the right to access and correct their information.

What protection is there for consumers' Social Security numbers?

Social Security numbers are often referred to as the keys that unlock consumers' identities, yet protection for this valuable information is woefully inadequate. Originally intended for calculating individuals' Social Security benefits, Social Security numbers are now used to identify people for many other purposes, from health insurance records to credit files to utility accounts. The widespread use of Social Security numbers increases their exposure and potential to be stolen by identity thieves. Some states, such as California, limit the use of Social Security numbers.

However, there is no federal law that restricts asking for consumers' Social Security numbers, using them as identifiers (except for a 2004 federal law that prohibits states from putting Social Security numbers on drivers' licenses or other state IDs[50]) or selling them, nor is there any federal requirement that Social Security numbers be securely

---

[46] See http://www.oispp.ca.gov/consumer_privacy/consumer/documents/pdf/cis8englsih.pdf
[47] For example, see identity theft passport information from Ohio Attorney General's Office, http://www.ag.state.oh.us/victim/idtheft/victim_assistance_kit.pdf
[48] See Privacy Rights Clearinghouse fact sheet, *Employment Background Checks: a Jobseeker's Guide*, http://www.privacyrights.org/fs/fs16-bck.htm#5
[49] See Privacy Rights Clearinghouse, *Online Data Vendors*, for lists of companies that offer consumers' personal information online and their opt-out policies, http://www.privacyrights.org/ar/infobrokers.htm
[50] See Social Security Legislative Bulletin, January 7, 2005, http://www.ssa.gov/legislation/legis_bulletin_010705.html

safeguarded. The President's Identity Theft Task Force has recommended that government agencies reduce the use of Social Security numbers[51] and the FTC has issued recommendations concerning use of Social Security number by the private sector to reduce the potential for identity theft.[52]

When an identity thief steals someone's Social Security number, resolving the problem is much more difficult than when a financial account number is compromised. While it is possible to change Social Security numbers, it is not advisable to do so except in extreme cases since they are now used as identifiers for so many fundamental purposes.[53] Victims can report that someone is fraudulently using their Social Security numbers to the Social Security Administration, but that will not necessarily stop the identity thief from continuing to use their Social Security numbers. Victims should check their Social Security Statements regularly and dispute any information that is inaccurate. They can obtain their statements by calling 1-800-772-1213.

Identity Theft Services Examined in CFA Study

The descriptions we provide for these services are based on the information on their Web sites, phone conversations that we had with some of the companies' customer service personnel, and publicly available information. The features, costs, terms and conditions and other aspects of these services are subject to change at any time. CFA began this research in September 2008 and re-checked the services' Web sites in February 2009, but it is possible that there have been changes since then.

These are not the only identity theft services available, but they are a representative sample of what is currently offered in the marketplace. The descriptions that follow are based mostly on the information available on the services' Web sites; when necessary we called the companies' customer service numbers or sent emails as a consumer to ask for more information or clarification. These services are discussed in much more detail about later in this report.

---

[51] *The President's Identity Theft Task Force Report*, September 2008, http://www.idtheft.gov/reports/IDTReport2008.pdf

[52] *Security in Numbers, SSNs and Identity Theft*, December 2008, http://ftc.gov/os/2008/12/P075414ssnreport.pdf

[53] The Privacy Rights Clearinghouse provides detailed information about Social Security numbers at http://www.privacyrights.org/fs/fs10-ssn.htm and http://www.privacyrights.org/fs/fs10a-SSNFAQ.htm

Company	Consumerinfo.com (an Experian company)
Service	ProtectMyID.com™
URL	www.protectmyid.com
Cost	$9.95 per month (12 months would total $119.40), option to purchase protection for children for an extra fee
Monitoring	▪ Files at all three credit bureaus ▪ Alerts by email
Other Features	▪ Access to Experian credit report ▪ Lost wallet feature enables customers to register credit, charge, debit and ATM cards with service and get assistance replacing them if lost or stolen ▪ Reimburses customers for unauthorized charges or debits they may have to pay as result of identity theft
Victim Assistance	Dedicated "Identity Theft Resolution Professionals" available 24/7, extent of assistance provided not clear from Web site or by talking to customer service representative
Guarantee/Insurance	Guarantee up to $1 million

Company	Equifax
Service	ID Patrol™
URL	www.equifax.com, click on "view all products," and click on specific service
Cost	$14.95 per month (12 months would total $179.40)
Monitoring	▪ Files at all three credit bureaus; scans Internet for customers' Social Security numbers and other personal information on "underground" Web sites identity thieves use to buy and sell information (customers can provide up to 10 credit card numbers to be monitored) ▪ Alerts by email or text message
Other Features	▪ Customers can "lock" and "unlock" their Equifax files quickly online ▪ Unlimited access to Equifax report, free "3-in-1" report
Victim Assistance	"Identity Theft Resolution Specialists" available 24/7, extent of assistance provided not clear from Web site, customer service representative told us that they provide advice
Guarantee/Insurance	Insurance up to $20,000 from Traveler's Casualty and Surety

Company	TransUnion
Service	TrueCredit™
URL	www.truecredit.com
Cost	$14.95 (12 months totals $179.40)
Monitoring	▪ Files at all three credit bureaus ▪ Alerts by email
Other Features	▪ Unlimited access to credit reports and scores from all three credit bureaus ▪ Customers can "lock" and "unlock" TransUnion files quickly online
Victim Assistance	Fraud assistance available 24/7, extent of assistance provided not clear from Web site, customer service representative told us that they provide advice
Guarantee/Insurance	Insurance up to $25,000 from AIG

Company	Identity Theft Assistance Center
Service	ITAC Sentinel®, ITAC Sentinel Plus®, ITAC Sentinel Premium®
URL	www.itacsentinel.com
Cost	Sentinel $9.99 per month (12 months totals $119.88) or $99.90 prepaid for one year Sentinel Plus $12.99 per month (12 months totals $158.88) or $129.90 prepaid for one year Sentinel Premium $17.99 per month (12 months totals $215.88) or $179.90 prepaid for one year
Monitoring	▪ Basic service monitors Equifax files; scans Internet black market for credit card numbers that customers register ▪ Two higher levels of service monitor customers' files at all three credit bureaus ▪ Premium also searches for customers' information in public records, Internet chat rooms and news groups ▪ Alerts by email or mail
Other Features	▪ Basic service provides quarterly updates of Equifax files and credit scores ▪ Higher levels of service provide quarterly reports and credit scores from all three credit bureaus
Victim Assistance	Assistance available 24/7, notifies law enforcement agencies, credit bureaus, creditors and others as necessary on behalf of victims to help them resolve their problems
Guarantee/Insurance	▪ Basic service provides insurance up to $2,500 (with $250 deductible) from Traveler's Casualty and Surety ▪ Insurance up to $20,000 for higher levels of service

Company	Intersections, Inc.
Service	Identity Guard Total Protection®
URL	www.identityguard.com
Cost	$14.99 per month (12 months totals $179.88)
Monitoring	▪ Files at three all credit bureaus; public records; Internet black market for credit card and bank account numbers that customers register; databases for credit applications in customers' names ▪ Alerts by email, text message, mail or phone
Other Features	▪ Quarterly updates to "3-in-1" credit reports and scores ▪ Several security features including encryption program to prevent "keyloggers" from capturing passwords and other information and "ID Vault Personal Password Protector" to securely store customers' user names and passwords ▪ Lost wallet assistance
Victim Assistance	Dedicated staff available 24/7, provides advice
Guarantee/Insurance	Insurance up to $20,000 (with a $250 deductible) from Travelers Casualty and Surety

Company	Prepaid Legal Services
Service	Identity Theft Shield™, Identity Theft Shield Gold™
URL	www.prepaidlegal.com/newCorp2/legal_plans/idt_shield.html
Cost	▪ Basic $12.95 per month (12 months totals $155.40) plus $10 enrollment fee ▪ Gold $15.95 per month (12 months totals $191.40) plus $10 enrollment fee ▪ Discounts for consumers who also subscribe to legal plans
Monitoring	▪ Basic service monitors Experian files ▪ Gold monitors the files at all three credit bureaus ▪ Alerts by email or mail
Victim Assistance	Available from Kroll Background America 24/7, no details provided on Web site; customer service representative told us that in addition to providing advice, fraud assistance personnel "handle everything" that needs to be done to resolve identity theft problems if customer signs power of attorney agreement

Company	Trilegiant Corporation
Service	IdentitySecure
URL	www.identitysecure.com
Cost	$14.99 per month (12 months totals $179.88)
Monitoring	▪ Files at all three credit bureaus; public records; scans underground Web sites, chat rooms and blogs for credit and debit card numbers that customers register; monitors Web sites for customers' Social Security numbers; checks online directories and search engines for changes in customers' addresses, email address and telephone numbers ▪ Alerts by email or mail
Other Features	▪ "3-in-1" credit report and score, toll-free number customers can call for help understanding credit reports ▪ Many other features including loan payment calculators, lost wallet assistance, access to DMV records, Medical Information Bureau report and Social Security report, computer security tools, personalized identity theft risk score ▪ Alerts by email or mail
Victim Assistance	▪ Online "Fraud Assistance Toolbox" provides advice about how to resolve customers' specific identity theft problems ▪ Online history file keeps track of steps customers have taken, follow-up email reminder sent about next steps ▪ Fraud assistance personnel available by phone or email 8 a.m. to midnight EST if customers need more advice
Guarantee/Insurance	Web site says insurance up to $10,000 from Virginia Surety Company; customer service representative told us it was up to $25,000

Company	ID Theft Assist LP
Service	ID Theft Assist
URL	www.idassistonline.com
Cost	$149.95 per year includes spouse/domestic partner, children under age 21 living at home, children under age 24 who are full time students
Monitoring	▪ Customers may activate credit monitoring option if desired, customer service representative told us that it is only TransUnion files currently (customers can purchase 3-bureau monitoring at discounted price) ▪ Annual fee only includes credit monitoring for one person; monitoring for others in household available for extra charge ▪ Alerts sent by email or mail
Other Features	TransUnion credit report; customers can buy "3-in-1" reports and scores for discounted price
Victim Assistance	▪ Fraud assistance available 24/7, sends victims "ID Theft Emergency Response Kit" and ID Theft Affidavit and Authorization Form, contacts credit bureaus, creditors, government agencies, law enforcement authorities on their behalf to resolve their problems ▪ Provides legal consultation but no reimbursement for legal or other expenses ▪ Translation services provided if needed

Company	Intelius
Service	IDWatch
URL	www.intelius.com/id-watch.htm
Cost	$9.95 per month for 3 months prepaid ($29.85); $7.95 per month (minus current 25% off special) prepaid for one year ($95.40); $4.95 per month prepaid for three years ($171.20)
Monitoring	▪ Creates "Identity Profiles" for customers to determine if they are already identity theft victims and form baseline for monitoring ▪ Monitors public and private databases for changes in profile; Internet "black market" for sale of personal information ▪ Alerts by email
Other Features	▪ Customers can go online to view alerts they have received ▪ Customers can purchase updated identity profiles, no information provided about the charge for this
Victim Assistance	"ID Theft Specialists" available 24/7, send victims "Identity Theft Recovery Kit" and provide advice
Guarantee/Insurance	Insurance up to $25,000 provided (unclear where the insurance is from, no response to email asking that and other questions)

	ID Watchdog
Service	ID Watchdog
URL	www.idwatchdog.com
Cost	$19.95 per month (12 months totals $239.40) plus $1.95 initial fee to verify identity of applicant; or $179.95 prepaid for one year, $359.95 for three years, with no verification fee; family plan also available
Monitoring	▪ Creates "Baseline Identity Profiles" for customers to determine if they are already identity theft victims and form baseline for monitoring ▪ Monitors files at all three credit bureaus, public and private databases for changes in profile; Internet "black market" for sale of personal information ▪ Alerts customers by email or mail ▪ If customers approve new information about them, it is added to their profiles; if they respond that they don't recognize the information (or there is some other indication of possible identity theft) company prepares more comprehensive "ID Snapshot" report to determine if there is an identity theft problem and what needs to be done to resolve it
Victim Assistance	▪ Fraud resolution personnel available 7 a.m.-5 p.m. PST, Monday through Friday ▪ Once victims obtain police report and sign ID Theft Affidavit and power of attorney, company takes whatever action is necessary on their behalf to resolve their problems ▪ ID Snapshot and resolution services included in the cost of membership for identity theft that occurs after enrolling; if initial identity profile reveals that consumer is already an identity theft victim, or if consumer knows that at time of enrollment, ID Snapshot and resolution services can be purchased for additional fees ($99.95 for ID Snapshot, $79.95 per fraudulent incident for the resolution services)
Guarantee/Insurance	Company guarantees to resolve customers' identity theft problems for them (no reimbursement for expenses or losses)

Company	Privacy Matters™
Service	Privacy Matters Identity™
URL	www.privacymatters.com
Cost	$29.95 per month (12 months totals $359.40)
Monitoring	▪ Creates personal identity profiles for customers to determine if they are already identity theft victims and form baseline for monitoring ▪ Monitors files at all three credit bureaus, public and commercial databases for changes in profile ▪ Alerts customers by email or phone
Other Features	▪ Customers can monitor profiles online ▪ Online tools to learn about credit, assess finances ▪ "ID Theft Score," advice about how to reduce risk
Victim Assistance	Assistance available 24/7, Web site says that "licensed investigators will work to help restore your name as effectively and efficiently as possible;" customer service representative could not tell us exactly what they do or whether help with preexisting problems is provided

Company	IdentityTruth
Service	IdentityTruth®
URL	www.identitytruth.com
Cost	$9.99 per month (12 months totals $119.88) with 3 month minimum; $99 prepaid for one year; $229.99 prepaid for 3 years
Monitoring	▪ Creates personal identity profiles for customers to determine if they are already identity theft victims and form baseline for monitoring ▪ Monitors files at all three credit bureaus, public and private databases for changes in profile; Internet black market for sale of personal information ▪ Alerts by email
Other Features	▪ Credit report from Experian ▪ Notice of security breaches (all known breaches, does not determine whether they are relevant to customer) ▪ Removal from pre-approved credit and insurance offers ▪Dynamic "Identity Health Score" measures risk
Victim Assistance	"Trained specialists" available 24/7 for advice and assistance, extent of assistance provided not clear from Web site; customer service representative told us that they will contact creditors and others on victims' behalf if needed (but not for pre-existing identity theft problems)
Guarantee/Insurance	Customer service representative said insurance up to $25,000 provided; we could not find this on Web site

Company	LifeLock®
Service	LifeLock®
URL	www.lifelock.com
Cost	$10 per month for adults (12 months totals $120) or $110 prepaid for one year; $2.50 per month (12 months total $30) or $25 per year for children under age 16 with adult enrollment
Monitoring	▪ Scans underground Web sites for customers' Social Security numbers, credit card numbers and other personal information ▪ Monitors address databases for new address information associated with customers
Other Features	▪ Places initial fraud alerts on all customers' files at the three credit bureaus, automatically renews them every 90 days ▪ Lost wallet assistance ▪.Requests free annual reports from all three credit bureaus ▪ Removes customers from the mailing lists for preapproved credit and insurance offers
Victim Assistance	Assistance available 24/7, extent of assistance not clear from Web site; customer service representative told us they provide advice, make three-way-calls to creditors with customers
Guarantee/Insurance	Company promises to spend up to $1 million to resolve customers' problems

Company	Debix, Inc.
Service	Identity Protection Network™ (adults), ChildScan® (children)
URL	www.debix.com
Cost	$24 per year for adults, children's service $20 per year per child
Monitoring	None for adults; children's service searches public and private databases for possible fraudulent use of child's Social Security number and notifies parents
Other Features	▪ Places fraud alerts on all customers' files at the three credit bureaus, automatically renews them every 90 days ▪ Assigns special Debix phone number for customer and includes it in fraud alerts; if creditor calls number to verify identity of person applying for new account, Debix makes automated call to customer, who can approve transaction using PIN number or press star key to deny approval as fraudulent
Victim Assistance	▪ If customers deny approval of transaction as fraudulent, they are immediately connected to "OnCall Investigation Team," which gathers information and provides it to law enforcement agencies ▪ Victims have access to customer service 24/7 for advice about what to do to resolve identity theft problems and receive "ID Theft Recovery Kit"
Guarantee/Insurance	Insurance from AIG (no amount specified, customer service representative told us it is up to $25,000)

Company	TrustedID®
Service	ID Freeze®
URL	www.trustedid.com
Cost	$10 per month for individuals with 3 month minimum (12 months totals $120); $19.99 per month for families with 3 month minimum (12 months totals $239.88); or $99 prepaid for one year for individuals, $189.99 for families
Monitoring	▪ Monitors public records; scans black market Web sites for customers' information for sale ▪ Alerts by email
Other Features	▪ Places "fraud flags" (fraud alerts) on all customers' files at the three credit bureaus, automatically renews them every 90 days ▪ Requests free annual reports from the three credit bureaus ▪ Lost wallet assistance ▪ Removes customers from mailing lists for preapproved credit and insurance offers and other unspecified marketing lists ▪ Provides spyware software ▪ Helps customers review medical benefit statements
Victim Assistance	"On-Call Protection Specialists" available Monday-Friday, 9-6 CST, provide advice, send victims claims kit, notify creditors, law enforcement agencies, others on their behalf per warranty
Guarantee/Insurance	Limited warranty up to $1 million

Company	One You Security, LLC
Service	Suite of services includes One You FraudWatch, One You PowerScan, One You MailWatch, One You PrivacyWatch
URL	www.oneyou.com
Cost	$10 per month (12 months totals $120) or $99 prepaid for one year for individual; $20 per month (12 months totals $240) or $149 prepaid for one year for individual and spouse/partner; each child $2.50 per month (12 months totals $30) or $25 prepaid for one year
Monitoring	▪ PowerScan searches underground Web sites, chat rooms, message boards and blogs for customers' personal information ▪ MailWatch monitors national address change databases for changes in customers' addresses ▪ Alerts by email
Other Features	▪ FraudWatch places fraud alerts on all customers' files at the three credit bureaus and renews automatically every 90 days ▪ Removes customers from unspecified mailing lists ▪ Customers receive free credit report periodically, not clear which ones or whether they are free annual reports
Victim Assistance	Promises to resolve problems with new credit accounts fraudulently opened in customers' names per guarantee
Guarantee/Insurance	Guarantee up to $1 million

Key Problems Uncovered by CFA Identity Theft Service Study

Failing to Provide Clear, Complete Information about the Services

To evaluate whether to buy identity theft services and make comparisons, consumers need to know exactly what they do and how they work. Clear, complete information should be provided on the Web sites and available from customer service representatives. We found that this was not always the case.

What is monitored?

Some services that provide monitoring do not make clear exactly what they monitor. For instance, the ID Theft Assist Web site says the service provides free credit monitoring but does not say that it is only TransUnion files. IDWatch says that the "Identity Profile" it creates for the customer contains information "including a current credit report"[54] but does not specify which report or explain whether it monitors the files at any of the credit bureaus; we were not able to get through by telephone and received no response to our email asking that question. Identity Theft Shield does not make clear that the "regular monitoring of your credit report" included in its basic plan is only your Experian report. IdentityTruth told us that it monitors all three credit bureaus, but does not explicitly state that on the Web site.

While it may not be practical – or wise – to list every database that they monitor, identity theft services should at least disclose whether credit bureaus are included, and if so, which ones. That information would help consumers decide which reports to request on their own, how often to request them, and what other steps they may wish to take to monitor their credit reports.

Another piece of information that is sometimes missing in describing monitoring services is how consumers are alerted if any changes or suspicious activities related to their personal information are detected. Most send alerts by email, but some provide other options for consumers who don't have email or prefer to receive their alerts another way.

What fraud resolution services are provided?

Most of the services we looked at provide some sort of assistance to customers if they become identity theft victims, but in many cases the extent of that assistance is not clear. For example, ID Patrol offers "24/7 access to ID Theft Resolution Specialists" but does not explain what they do; a customer service representative told us they provide advice.[55] Privacy Matters Identity says that "Licensed investigators will work to help restore your name as effectively and efficiently as possible,"[56] which makes it sound as if they take an

[54] https://www.intelius.com/id-watch.html?PHPSESSID=04d6f1ec3bfa8d6128eaa9de27490c2c, last accessed 2/26/09
[55] http://www.equifax.com/credit-product-list/, last accessed 2/26/09
[56] http://identity.privacymatters.com/member-benefits.aspx , last accessed 2/26/09

active role in resolving victims' problems, but the customer service representative was unable to answer our questions in that regard.

We found that in most of the services we examined, the fraud assistance consists of providing the customer with a kit of materials and advice about the steps that they must take themselves to resolve their problems. Identity Guard Total Protection describes this fairly well when it says that it "guides you through the process of recovery should you become a victim."[57]

Some services do take a more active role on behalf of victims. For instance, ID Watchdog explicitly states that it will do whatever is necessary on behalf of customers to resolve their identity theft problems[58] and ID Theft Assist also explains its resolution services fairly well.[59] But this information is not always clear. ITAC Sentinel, for example, contacts creditors, law enforcement authorities, and others on behalf of customers, but what it does and the limits of what it does are explained as well as they might be in the description of the service[60] or on the main ITAC Web site.[61]

The extent of the assistance provided to victims could be a major consideration in choosing an identity theft service. It should be clearly explained on services' Web sites and their customer service personnel should be able to answer questions in that regard.

We also found that the assistance the service provides to victims may not be available if they already have "pre-existing" identity theft problems. However, policies in this regard vary and consumers may have to look carefully at the terms of service or the details of the guarantees or insurance policies, if provided, to find that information (problems with guarantees and insurance are discussed in more detail later in this report).

ID Theft Assist explains in its terms of service that "any identity thefts or incidents discovered by the Covered Member prior to service effective date is ineligible for service,"[62] making it clear that if the incident occurred before the consumer enrolled but was not discovered until after, the resolution services will be provided. But many services do not adequately explain their policies. For instance, the terms and conditions for ProtectMyID state that it is not obliged to provide fraud assistance for, among other things, "losses, damages or expenses that were incurred or commenced prior to the membership."[63] Does this mean that the service will not provide advice if the customer discovers after enrolling that an identity theft occurred before that time? We're not sure.

It is especially important for services that create "profiles" of customers when they enroll to disclose whether help is available to resolve pre-existing identity theft problems that may be uncovered in that process. ID Watchdog makes clear that you can purchase

[57] http://www.identityguard.com/GetProtected/landing.aspx , last accessed 2/26/09
[58] http://www.idwatchdog.com/guarantee.php, last accessed 2/26/09
[59] http://www.idassistonline.com/benefits_and_services.php, last accessed 2/26/09
[60] http://www.itacsentinel.com/Sentinel.aspx, last accessed 2/26/09
[61] http://www.identitytheftassistance.org/pageview.php?cateid=48, last accessed 2/26/09
[62] http://www.idassistonline.com/terms_of_service.php, last accessed 2/26/09
[63] http://www.protectmyid.com/terms/, last accessed 2/26/09

resolution services for pre-existing identity theft problems.[64] We could not find any information in this regard on the Web sites of IDWatch, IdentityTruth, or Privacy Matters. When we attempted to contact IDWatch by phone, we followed the prompts for general questions and were put on hold so long that we finally gave up. Consumers can also ask questions by email. We did so, but never received a response. The customer service representative at Privacy Matters was unable to answer that question. IdentityTruth told us that the company provides advice for customers with pre-existing identity theft problems but will not contact creditors and others on their behalf.

Whether assistance resolving pre-existing identity theft problems is provided and under what circumstances should be clearly explained, not just in the terms and conditions or details of insurance, which many consumers may not wade through, but in any references to fraud assistance on the services' Web sites. Customer service personnel should also be able to answer that question.

Services that offer access to fraud assistance personnel should also provide information on their Web sites about when they are available; not all do. It's not necessarily crucial for live help to be available 24/7, since consumers can easily take the most urgent steps, such as placing fraud alerts and notifying credit card issuers, themselves. But some consumers may want to consider that information in comparing services.

How much does the service cost?

Several of the identity theft services we examined do not provide information on their Web sites about how much the services cost until the consumer clicks on "Join."

Cost information should be on the home page so that consumers can easily compare this information from one service to another.

Placing Fraud Alerts on Consumers' Files

Some identity theft services place fraud alerts on customers' files as a preemptive measure. There are serious questions about the propriety of this practice. We are also concerned about the representations we found on some services' Web sites about when consumers are entitled to place fraud alerts on their files and what protection alerts offer.

Who can place fraud alerts?

The issue of whether identity theft services can legally place fraud alerts on behalf of consumers has been raised in lawsuits filed in 2008 against LifeLock. Both a suit by Experian[65] and class action suits brought on behalf of consumers[66] contend, among other

[64] http://www.idwatchdog.com/protect.php, last accessed 2/26/09
[65] Experian Information Solutions, Inc. v LifeLock, Inc., U.S. District Court for the Central District of California, Case No. SACV08-00165

things, that the FCRA only allows a consumer or an "individual" acting on behalf of the consumer to request an initial fraud alert.[67] They further argue that it is clear from the legislative history of the statute that the word "individual" was intentionally used instead of "person" (which many laws and regulations define as including a business) to preclude credit repair services and other companies from placing these alerts for consumers and charging them to do so.[68]

In addition, Experian says that the fraud alert placement system is designed specifically for consumers to do themselves, following prompts that request certain information from them. It accuses LifeLock of falsely pretending to be the consumers when it calls Experians's toll-free fraud number to place fraud alerts on their files.

Experian also asserts that Lifelock's spurious placement of fraud alerts causes credit bureaus to incur significant expenses to process and respond to them, dilutes their impact, and increases the likelihood that consumers who are legitimately applying for credit will be denied. In addition Experian says that repeated applications and denials caused by unnecessary fraud alerts can harm consumers' credit scores.

When can the initial fraud alerts be placed?

The Experian and class action suits against LifeLock also claim that the company violates the FCRA by submitting requests for initial fraud alerts where there is no good faith suspicion that the customer has been or is about to become a fraud victim and that LifeLock makes many misrepresentations in promoting its services, including the extent of the protection that the initial fraud alerts and its guarantee provide (guarantees are discussed later in this report). We found troublesome claims on LifeLock's Web site regarding when consumers are entitled to place fraud alerts, including:

> "Our job is to protect your good name. As a consumer, you have rights that allow you to take more control over who uses your identity and how they use it. We do the mechanics, the details if you will, to enforce those rights."[69]

This reference to LifeLock's placement of fraud alerts makes it sound like all consumers are entitled to request them, when that right is intended only for people who have reason to believe that they are or may imminently be victims.

Debix also implies that everyone has the right to place a fraud alert, regardless of their victim status, when it says in the "How It Works" section of its Web site:

---

[66] These class action cases, which were filed separately, are now combined as In re LifeLock, Inc., Marketing and Sales Practices Litigation, MDL Docket No. 08-1977-MHM, U.S. District Court for the District of Arizona

[67] 15 U.S.C. §1681c-1(a)

[68] See H.R. Rep. No 108-263 at 40 (September 4, 2003)

[69] http://www.lifelock.com/lifelock-for-people, last accessed 2/26/09

> "In 2003, Congress gave you the right to place a fraud alert on your credit files - notifying banks and creditors that they are not authorized to open new accounts without first verifying your identity."[70]

One You Security makes a similar contention when it says about its placement of fraud alerts:

> "We start where you have the most exposure. Making sure no one can open new credit in your name except you. We do this by placing and continually renewing a fraud alert* on your credit report. A fraud alert puts an extra step in the credit granting process requiring any company issuing new credit to you to contact you before processing the application confirming you are really the person applying for the credit. If the system were set up for you, instead of financial institutions and businesses, they would have built this into the credit approval process. But today you do have this right and we believe every American should take advantage of it."[71]

There is nothing that corresponds to the asterisk in this statement. We will address the claim about what the creditor will do when there is a fraud alert next in this report.

Are the claims about how fraud alerts protect consumers misleading?

We found many misleading claims about how the initial fraud alerts that are placed preemptively on consumers' files by some of the identity theft services we studied actually protect consumers from identity theft. For instance, LifeLock states that every time customers apply for new credit or someone "tries to do something" with their credit:

> **"**You should receive a phone call from the bank asking if you are actually the person applying for credit in your name. If you are, great. If not, the transaction stops."[72]

In fact, the initial fraud alerts that LifeLock places on consumers' files do not oblige banks to call them. Another section of the Web site says:

> "Who calls me to let me know that someone is attempting to obtain credit in my name?
> If someone is trying to use your personal information, you will be contacted by the creditor that is issuing the line of credit. If you receive a call and you are not the one applying for credit, the transaction should be stopped immediately."[73]

---

[70] http://www.debix.com/products_how_it_works.php, last accessed 2/26/09
[71] http://www.oneyou.com/OurSolution/tabid/58/Default.aspx#fraudWatch, last accessed 2/26/09
[72] http://www.lifelock.com/lifelock-for-people/what-we-do/how-does-lifelock-protect-my-identity, last accessed 2/26/09
[73] http://www.lifelock.com/1636, last accessed 2/26/09

But the creditor is not required to contact the consumer by phone or any other means, as this suggests.

There is an explanation of the initial fraud alerts that provides more accurate information:

> "After a fraud alert has been placed in your credit file, any creditor using that credit file to grant new credit or an extension of credit in your name should take reasonable steps to verify your identity and confirm the credit application is not the result of identity theft. This can be done by contacting you by phone, via the mail or by using other methods to verify the application is legitimate."[74]

But this information is counteracted by the other statements on LifeLock's Web site and by advertisements such as the full page ad that appeared in the *Arizona Republic* newspaper on March 7, 2008 which stated "LifeLock's proactive approach includes setting and maintaining alerts that force creditors to contact LifeLock customers directly before they can issue new lines of credit."

We were also troubled by statements that Debix makes about the initial fraud alerts that it places, such as:

> "Federal law requires banks and creditors contact you to verify your identity before opening a new line of credit."[75]

> "How do banks contact me?
> Debix assigns a secure phone number to your account and places that phone number in your credit file. When a bank reviews your credit file they will see your fraud alert and call your Debix phone number. Debix's secure voice server will answer and contact you immediately for approval."[76]

Other statements include:

> "The law outlines the best practice - placing a call to the number requested by a consumer - but stops short of absolutely requiring creditors to place a call and gives them the discretion to use 'other reasonable measures'…"

> "If a creditor elects not to call, utilizes "other reasonable measures", and opens an unauthorized account in your name, you are still protected with Debix…"

---

[74] http://www.lifelock.com/lifelock-for-people/how-we-do-it/what-is-a-fraud-alert, last accessed 2/26/09
[75] http://www.debix.com/products_how_it_works.php, last accessed 2/26/09
[76] http://www.debix.com/faq.php#q2, last accessed 2/26/09

> "Also, the Debix Audit Trail will demonstrate a call was not placed, and whatever action taken by the creditor was not "reasonable", because it resulted in fraud. Debix will then assist you in obtaining the greater level of protection which you are entitled to under the law and ensures consistent response from banks and creditors."[77]
>
> "Do all banks have to call me before opening new accounts?
> The Fair and Accurate Credit Transactions Act of 2003 states that all banks and creditors must call you before opening new credit accounts. However, there are exceptions and some creditors still ask personal questions or send letters requesting additional verification. In all cases, they must take extra precaution to make sure the credit application is not the result of identity theft. If a creditor opens a fraudulent account without calling you first, Debix can provide a record demonstrating that the creditor failed to honor your right to a phone call and use that record to speed the recovery process."[78]

We have several concerns about these statements. First, as we have said, there is no obligation to call or contact the consumer in any other way. Second, the language of the FCRA does not appear to suggest that calling the consumer is the best way to verify the credit applicant's identity. It says "If a consumer requesting the alert has specified a telephone number to be used for identity verification purposes, before authorizing any new credit plan or extension described in clause (i) in the name of such consumer, a user of such consumer report shall contact the consumer using that telephone number or take reasonable steps to verify the consumer's identity and confirm that the application for a new credit plan is not the result of identity theft."[79] In other words, if the consumer who places a fraud alert provides a phone number for verification and the creditor decides to call, that's the number it should use. The alternative of taking other reasonable steps seems to be given equal weight.

Furthermore, the fact that an identity thief succeeds in obtaining credit in the consumer's name, despite the initial fraud alert, does not prove that the creditor failed to take reasonable measures. The identity thief might have provided the additional information requested. And some creditors don't even check credit reports; the requirements related to fraud alerts apply only if they do.

Debix works with creditors to encourage them to call consumers when they see phone numbers provided with initial fraud alerts, an effort that we applaud. However, if consumers fall victim to identity theft, their ability to get the problems resolved promptly does not hinge on being able to prove whether the creditor called or not, nor does their right to obtain a greater level of protection by placing extended alerts on their files.

---

[77] id
[78] http://www.debix.com/faq.php#q1, last accessed 2/26/09
[79] 15 U.S.C. § 1681 c-1 (h) (1) (B) (ii)

We were pleased to see that since we first looked at the TrustedID's Web site in September 2008 the explanation about the "fraud flag" feature in IDFreeze no longer states that it requests creditors contact consumers before taking any action that may affect their credit.

However, the description of One You FraudWatch on One You Security's Web site still makes some misleading claims about the protection that the initial fraud alerts it places on customers' files provide, including:

> "First we initiate a fraud watch, which enables fraud alerts on your personal credit. We make sure that no one but you can open new credit in your name."[80]

Placing the fraud alerts does not ensure that an identity thief will be unable to open a new credit account in a consumer's name.

> "What is a fraud alert? A fraud alert is placed on your credit report at the three major credit bureaus requiring any company issuing you new credit to first contact you and confirm you are really the person applying for the credit. It's a check in the system intended for anyone who has been or thinks they may become a victim of identity theft."[81]

There is no obligation to contact the consumer, and while many people are worried that they might become identity theft victims, the FCRA requires that there must be "a suspicion that the consumer has been or is about to become a victim of fraud" to request a fraud alert – a much more specific criteria than the company's description of a fraud alert suggests. In fact, in the Frequently Asked Question the company says:

> "Why would I think I may become the victim of identity theft? Since 2005 there have been over 225 million data breaches containing personal information on individuals in this country. Your Social Security Number is the key to your financial kingdom. You use this number to get a cell phone, go to the doctor, get a job, and receive a mortgage or bank loan. You can't function in society without giving it out on a regular basis. It's everywhere and easy for identity thieves to get. Anyone who has a Social Security Number is a prime candidate to become a victim of identity theft."[82]

The number of data breaches that have occurred, while alarming, is not a valid reason for someone to request a fraud alert (but notice of a breach affecting the person would be), nor is *anyone* who has a Social Security number a likely victim.

---

[80] http://www.oneyou.com/, last accessed 2/26/09
[81] http://www.oneyou.com/FAQs/tabid/63/Default.aspx, last accessed 2/26/09
[82] id

Are consumers being asked to lie about being fraud victims?

Another allegation in the Experian lawsuit against LifeLock is that the company misleads consumers to believe that that they are eligible for fraud alerts by asking them in the enrollment process to state why they think they will be become victims of identity theft and presenting them with choices that include "I have heard media reports that give me a reason" and "One of my friends or family members is a victim of identity theft." [83]

We found a similar drop-down menu in the enrollment section of One You Security's Web site that asks consumers this question and presents several choices, some of them valid reasons for requesting a fraud alert, such as "A company/organization who has my personal information had a data breach" and some that seem overly vague, including "I have several reasons."[84]

Furthermore, consumers may not realize that buried in the terms and conditions for LifeLock, Debix, and OneYou Security they are agreeing to assert that they are fraud victims in order to obtain the benefits of the fraud alerts that will be placed on their behalf. We're not sure how many consumers read this information or understand it. TrustedID's terms and conditions state that by enrolling in IDFreeze consumers are instructing the company to "fraud flags" on their files pursuant to a power of attorney agreement, which we could not find on the site.[85]

Should consumers who want creditors to take extra precautions before granting credit in their names be able to make that request even though they have no real reason to suspect that they are or are about to become victims? Should they be entitled to the type of protection that extended alerts, which specifically require creditors to contact consumers for verification, provide? These are questions that should be addressed by policymakers.

Solutions such as Debix's automated alert and response system can help to deter some types of new account fraud and should be available without consumers having to falsely assert that they are fraud victims.

Identity theft services should describe fraud alerts accurately and not overstate or make misleading claims for the protection they provide.

Failing to Provide Details of Insurance Coverage

Many identity theft services offer insurance as part of the membership package. These policies, provided by insurance companies, generally provide limited reimbursement for certain expenses that consumers may incur to resolve identity theft victims, such as lost wages if the victim had take unpaid time off from work to resolve an identity theft problem; legal expenses to defend themselves in suits and criminal actions resulting from identity theft; and miscellaneous expenses such as fees for re-filing loan applications,

[83] https://secure.lifelock.com/enrollmentform.aspx, last accessed 2/26/09
[84] https://www.oneyou.com/tabid/70/Default.aspx, last accessed 2/26/09
[85] https://www.trustedid.com/terms_conditions.php, last accessed 2/26/09

long distance telephone calls, notary fees, and postage. The total amount of reimbursement may be per identity theft incident, per year, or for the entire time that the consumer is enrolled in the service. Certain restrictions or requirements may apply. For instance, lost wages may be limited to a certain number of weeks and/or dollar amount. Victims may be required to seek prior approval to hire attorneys or investigators, which are sometimes provided for.

Pre-existing identity theft problems may not be covered or may be covered only under certain circumstances. In order to be eligible for reimbursement under an insurance policy, customers may have to follow specific instructions such as providing notice within a certain time of discovering the identity theft problem, filing a police report, and documenting expenses. Consumers should also be aware that the insurance coverage offered may not be available in their states due to state insurance regulations.

Of the eight services we examined that offer insurance, only IdentitySecure provides the full terms of the coverage on its Web site. Some services provide the highlights of the insurance coverage. For example, TrueCredit states that the policy included with its service covers lost wages up to $1,000 per week for a maximum of five weeks, legal defense expenses, fees to re-file loan applications, notary costs, long distance phone calls and postage.[86]

ID Patrol, on the other hand, only states the total amount of reimbursement and that "certain limitations and exclusions apply.[87] A customer service representative at IdentityTruth told us that insurance up to $25,000 was included, but there was no mention of that at all on the Web site. We found that customer service representatives were generally unable to provide details about what the insurance covers and the limitations, exclusions, or requirements that may apply.

Insurance policies may vary depending on the state in which the consumer lives; for instance, IdentitySecure's policy contains a special clause pertaining to residents of Montana. There is no reason why other identity theft services that offer insurance should not be able to provide the same type of information. CFA believes that insurance is of little value and consumers should not regard it as an important factor in choosing an identity theft service. However, if insurance is offered as part of the service, the terms should be provided upfront.

Identity theft services promote insurance as an important benefit. They should provide consumers with the details of the coverage upfront so they can assess how the insurance policies would benefit them or compare one to another. Customer service personnel should be able to answer questions about the insurance coverage.

[86] http://www.truecredit.com/popup/idTheftInsurancePopup.jsp?popup=true, last accessed 2/26/09
[87] http://www.equifax.com/id-patrol/, last accessed 2/26/09

Guarantees Failing to Provide the Protection Consumers may Expect

We found that information about guarantees that some identity services provide was usually more complete than the information about insurance. However, sometimes the details of the guarantees reveal that they provide much less protection than consumers may expect.

Some guarantees provide reimbursement for the same types of expenses that insurance policies cover. For instance, ProtectMyID's guarantee[88] reimburses for lost wages, legal defense fees and private investigators as needed (with advance approval), and miscellaneous expenses to resolve identity theft problems that occur while the consumer is a customer. It also reimburses customers for money stolen from any accounts that appear on their Experian credit reports (most guarantees or insurance do not appear to provide reimbursement for stolen funds, but as we explained previously, consumers are usually not liable for fraudulent debits from their accounts).

In some cases, the guarantee promises that the company will resolve the customer's identity theft problem at its own expense. For example, ID Watchdog's guarantee is to resolve customers' identity theft problems.[89] It also plainly states that no reimbursement for expenses or losses is provided.

One You Security's guarantee, on the other hand, is confusing and seems to be more limited than consumers may realize. On the home page, the company states:

> "We are so confident that our services will protect you from identity theft, that we back up every customer with a $1,000,000 service guarantee."[90]

The Frequently Asked Questions provide more information:

> "How does your $1,000,000 guarantee work? Our $1,000,000 service guarantee is in place to reimburse you for any actual out of pocket expenses or losses you suffer as a result of an identity theft while you are our customer. The average identity theft can take hundreds of hours and cost in excess of $1,000 to restore. While you're our customer, this will not be your burden to bear. It is our guarantee to you."[91]

But another section of the Web site begins to hint at the limits of the guarantee:

> "$1,000,000 Service Guarantee and Full Restoration Services
> One You Security can not absolutely guarantee that we can stop identity

---

88 http://www.protectmyid.com/Message.aspx?PageTypeID=MemberGuarantee&SiteVersionID=815&SiteID=100302&sc=668734&bcd=, last accessed 2/26/09

89 http://www.idwatchdog.com/guarantee.php, last accessed 2/26/09

90 http://www.oneyou.com/, last accessed 2/26/09

91 http://www.oneyou.com/FAQs/tabid/63/Default.aspx, last accessed 2/26/09

> theft from happening to you and neither can any other company. What we can absolutely guarantee you though, is if an identity thief *commits new account fraud in your name* (emphasis added) while you're our customer, it is not your problem. It is our problem. We provide you with a $1,000,000 service guarantee that covers you for any actual expenses you incur as a result of the incident…"[92]

In contrast to that statement, a more detailed description of the guarantee begins by saying that "One You Security's promise to you is no one is going to steal your financial identity while you're our customer."[93] But it goes on to explain that in the event that happens – specifically if an identity thief obtains credit in the customer's name – the company will spend up to $1 million to take the action necessary to resolve the problem.

The only reference to reimbursement we could find in this description of the warranty or in the terms and conditions to which it refers[94] is "We will not pay for or reimburse fees of professionals or other service providers unless we decide they are necessary and we select them." It was not clear from speaking with a customer service representative whether and under what circumstances reimbursement would be provided. However, the person did confirm that the guarantee only applies to situations in which an identity thief opens a new credit account using the customer's personal information.

LifeLock also promotes its $1 million guarantee as a major sales point. In the information about how LifeLock works, the guarantee is described thus:

> "If your Identity is stolen while you are a member of LifeLock, we're going to do whatever it takes to recover your good name. If you need lawyers, we're going to hire the best we can find. If you need investigators, accountants, case managers, whatever, they're yours. If you lose money as a result of the theft, we're going to give it back to you. We will do whatever it takes to help you recover your good name and we will spend up to $1,000,000 to do it. We don't think you will see a guarantee like this anywhere else from any other company. If you do, let us know because we'd like to do business with them. There isn't much fine print in our Guarantee. To see the details, click here."[95]

But if consumers click on the details and read them very carefully, they may be surprised to find that the guarantee is much more limited than they think. It says that if the customer's personal information is used to commit a fraud "*due to a failure or defect in our service*" (emphasis added) the company will pay professionals up to $1 million to recover the customer's losses.[96]

---

[92] http://www.oneyou.com/OurSolution/tabid/58/Default.aspx#millionGuarantee, last accessed 2/26/09
[93] http://www.oneyou.com/OurSolution/OurGuarantee/tabid/64/Default.aspx, last accessed 2/26/09
[94] http://www.oneyou.com/tabid/77/Default.aspx, last accessed 2/26/09
[95] http://www.lifelock.com/lifelock-for-people?oplisting=1, last accessed 2/26/09
[96] http://www.lifelock.com/our-guarantee, last accessed 2/26/09

According to the class action lawsuits against LifeLock, this means that the guarantee only applies to identity theft resulting from the company's failure to place a fraud alert on the customer's file or remove the customer from pre-approved credit marketing lists as promised. In other words, if LifeLock performs those services and identity theft occurs anyway, the customer has no recourse under the guarantee.

TrustedID's Web site proclaims that:

> "We are confident that your identity is better protected with TrustedID. As part of our commitment to you, we back our service with a $1,000,000 service warranty to cover out-of-pocket expenses in the rare event identity theft happens."[97]

But when one reads the terms of the warranty, what it promises is that the service will "perform substantially in accordance with any written specifications provided to You by TrustedID during the entire term of Your subscription"[98] and, if fails to do so and the customer suffers from identity theft as a result, reimbursement and restoration services will be provided. This sounds very similar to LifeLock's guarantee and it is not clear if customers are covered if they become identity theft victims even if the company has provided the services as promised.

Identity theft services that provide guarantees should describe them accurately and refrain from promising more protection and assistance than they actually provide. The fine print should supplement, not contradict, the claims made regarding guarantees.

Making Broad Assurances about Preventing Identity Theft

LifeLock's home page boldly states:

> "LifeLock, the industry leader in proactive identity theft protection, offers a proven solution that prevents your identity from being stolen before it happens."[99]

Todd Davis, the CEO of LifeLock, promotes this claim by providing his Social Security number in advertisements and on the Web site.[100] However, despite the claims that Davis makes about how the service protects him and other customers, his Social Security number was used by a man to obtain a $500 payday loan.[101] Apparently, the lender did not check Davis' credit report, but even if it had and saw a fraud alert, it is possible that the thief might have succeeded anyway if he was able to meet the verification requirements.

---

[97] https://www.trustedid.com/, last accessed 2/26/09
[98] https://www.trustedid.com/about_us.php?serviceterms=service_warranty, last accessed 2/26/09
[99] http://www.lifelock.com/?oplisting=0, last accessed 2/26/09
[100] http://www.lifelock.com/lifelock-for-people?oplisting=1, last accessed 2/26/09
[101] See http://today.msnbc.msn.com/id/24790921/

ProtectMyID makes a more realistic pitch:

> ProtectMyID.com™ offers a complete program for identity theft protection, detection and resolution to help you catch identity theft and fraud when it happens and reclaim your good name and credit if it does.[102]

IdentitySecure says it "offers an array of proactive measures that can help stop fraud before it occurs."[103] While it and many other services we examined may be able to alert consumers that their information is being offered for sale by identity thieves or that someone is already using their information, it cannot necessarily prevent fraud.

Phrases such as "total identity theft protection"[104] and "stop identity theft before it happens"[105] may give consumers a false sense of protection.

No identity theft service can prevent consumers' personal information from being stolen or used and none should imply that they can.

Charging Consumers for their Free Annual Reports

Many identity theft services provide customers with reports from one or all three credit bureaus as a benefit of membership. But instead of paying the credit bureaus for the reports, at least two of the services we examined, LifeLock, and TrustedID appear to obtain them by requesting the free reports that consumers are entitled to request once a year under the FCRA.

While this may be disclosed somewhere in the terms and conditions agreement – for instance, Lifelock's terms of service state that it will "order, upon enrollment and once a year thereafter, your annual credit reports from major consumer reporting agencies as may become appropriate, as permitted by 15 U.S.C. § 1681j (a)"[106] – consumers may not see this or understand what it means.

The Experian and class action lawsuits cited in this report contend that LifeLock misleads consumers by failing to adequately disclose that the credit reports it provides are the free annual reports that they are entitled to and that LifeLock's actions will prevent them from requesting the free reports themselves. Experian also asserts that, as with fraud alerts, only consumers or individuals acting on their behalf may request the free annual reports.

Identity theft services should be explicitly prohibited from requesting consumers' free annual reports on their behalf.

---

[102] http://www.protectmyid.com/, last accessed 2/26/09
[103] http://www.identitysecure.com/Content.aspx?content=why, last accessed 2/26/09
[104] See Privacy Matters Identity, http://identity.privacymatters.com/member-benefits.aspx, last accessed 2/26/09
[105] See TrustedID, https://www.trustedid.com/, last accessed 2/26/09
[106] http://www.lifelock.com/about-us/about-lifelock/terms-and-conditions, last accessed 2/26/09

Securing Consumers' Sensitive Personal Information

When consumers enroll in identity theft services they provide a good deal of sensitive personal information. In addition to providing their financial account numbers to pay for the services, they are usually asked for their Social Security numbers and other information that is needed to perform the monitoring, lost wallet assistance, and other services that are included in their memberships.

LifeLock makes this statement on its Web site about the security of customer's information:

> "LifeLock is ISO 27001 certified for data and operational security and follows industry best practices to secure and protect personal information. We conduct background checks on all of our employees, including regular random drug testing. All of our facilities are built with the latest biometric security access as well as state-of-the-art surveillance and alarm systems. No data is stored onsite. No computers anywhere outside of secure data centers have our member's critical information on them."[107]

However, among the class action suits against LifeLock, one asserts that these representations are false and misleading. It contends that the company hires third-party contractors who work remotely from their homes and have "unfettered" access to customers' Social Security numbers and other sensitive personal information, and that the company does not perform background checks on all of the third-party contractors that it employs.

We do not know if these allegations are true and neither we nor consumers have any way of assessing the security measures that identity theft services uses. But the question about security should be addressed.

Identity theft services should be required to take adequate measures to secure customers' information and should use independent auditors to ensure that they do.

Requiring Mandatory Binding Arbitration in Agreements

Half of the identity theft services we examined require in their terms of service that customers submit any disputes about this service to binding arbitration. Mandatory binding arbitration is aimed at preventing consumers from going to court if they believe that the company has misled them or failed to honor the promises it made. Since these agreements are one-sided, with no ability for the consumer to negotiate, we believe that requirements for mandatory binding arbitration are unfair.

Identity theft services should provide alternative dispute resolution as an option but not a requirement in their terms of service.

[107] http://www.lifelock.com/lifelock-for-people/how-we-do-it/how-does-lifelock-secure-my-personal-information, last accessed 2/27/09

Policy Recommendations

Government agencies, companies and industry groups, and consumer and privacy organizations have devoted considerable effort in the last several years on improving identity theft awareness and prevention. Over the same period, dozens of for-profit identity theft services have sprung up, offering to protect and assist consumers. The time has come to turn the focus on this industry. CFA's examination of for-profit identity theft services reveals questions and concerns that should be addressed by policymakers in government and business.

- The Federal Trade Commission and state attorneys general should examine the practices of for-profit identity theft services and take enforcement action to stop abuses, including misleading advertising about the services provided and how those services protect consumers, misleading claims about the guarantees provided and how those guarantees help consumers, and practices that harm consumers' credit reports and their ability to request their free annual reports.

- The Federal Trade Commission and state attorneys general should look into whether the sensitive personal information that consumers provide to identity theft services is adequately protected from internal or external abuse. Identity theft services should be required to take adequate measures to secure customers' information and should use independent auditors to ensure that they do.

- The Federal Trade Commission should promulgate rules governing the practices of for-profit identity theft services.

- The identity theft service industry should develop best practices to encourage companies to provide clear, complete information about their services and discourage unfair or deceptive practices.

- Identity theft services should be explicitly prohibited from requesting consumers' free annual reports on their behalf.

- All consumers should have the option to place a flag on their credit reports, at no charge, that would require creditors to contact them to verify applications for new credit accounts or changes to existing credit accounts in their names.

- Consumers should have the right to check their credit reports online, whenever and however frequently they choose, at no charge.

Appendix A

Ten Easy Steps to Protect Your Personal Information and Detect Fraud

1. **Practice mail security.** Use a public mailbox rather than your home mailbox to send bill payments and other mail containing sensitive information. Pick your mail up promptly and ask the post office to hold it while you're away.

2. **Guard your Social Security number.** Don't carry your Social Security card, military ID, Medicare, or other cards that have your Social Security number on them unless you are going somewhere where you will need them. Only provide your Social Security number when there is a legitimate need to do so.

3. **Lock and shred.** Keep your billing and banking statements and other personal records locked up and shred them when no longer needed.

4. **Stop prescreened credit and insurance mailings.** Call toll-free 1-888-567-8688 to get off mailing lists for credit and insurance offers. Your Social Security number will be required. This keeps thieves from intercepting and accepting the offers in your name and doesn't affect your eligibility for credit or insurance.

5. **Keep private information to yourself.** Never respond to phone calls or emails asking to confirm your Social Security number or account numbers. Don't leave PIN numbers, passwords or other personal information around for others to see.

6. **Be safe online.** Use anti-virus and anti-spyware software and a firewall on your computer and keep them updated. When you provide financial or other sensitive information online, the address should change from "http" to "https" or "shttp." A symbol such as a lock that closes may also indicate that the transmission is secure.

7. **Look at your bills and bank statements promptly.** If you find any charges or debits that you never made, contact the bank or company immediately.

8. **Monitor your accounts online frequently.** You can discover problems more quickly than if you wait for bills or statements to come by mail.

9. **Check your credit reports regularly.** You can get them free once every 12 months. Go to www.annualcreditreport.com, call 1-877-322-8228, or mail your request to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Your name, address, Social Security number, and date of birth will be required. You don't have to get your reports from all the consumer reporting agencies at once; you can stagger your requests throughout the year.

10. **Pay attention to debt collectors.** Calls or letters about overdue accounts you don't recognize could indicate identity theft. If you are contacted by the creditor, ask for documentation about the debt; if by a collection agency, explain that you dispute the bill and why (put it in writing to maintain your debt collection rights under federal law) and ask how to contact the creditor so you can investigate.

Appendix B

Six Questions to Ask When Shopping for Identity Theft Services

1. **Does it monitor more than credit reports?** Since it's easy to check your own credit report and you can access it once a year for free, and because many types of identity theft don't show up in credit reports, credit monitoring alone is of limited value. Consider services that scan other commercial databases, public records, rogue Web sites that sell stolen credit cards and Social Security numbers, and other places that may have your personal information and that aren't as easy for you to monitor yourself. Also check the options for receiving alerts; some services only send alerts by email, others offer more alternatives.

2. **How does the service help if you are a victim?** Most identity theft services only provide advice about the steps you'll need to take, but some take a more active role to help resolve your problems. Depending on the terms of service, assistance may be limited to identity theft that occurs, or is discovered, after you join. If it's unclear how the service will help you, continue to shop around.

3. **Will it prevent you from getting your free annual reports when you wish?** Credit reports are often provided to customers as part of identity theft services. But some companies obtain them by requesting the free reports that you are entitled to get once a year, effectively preventing you from exercising your right to ask for your free annual report when you want it.

4. **Should you look for identity theft services that offer insurance?** Insurance generally reimburses for lost wages if you must take time off from work without pay to resolve an identity theft problem, long-distance calls, postage, notary fees and other miscellaneous expenses. Money that an identity thief has stolen from you is usually *not* covered. Since most identity theft victims have little or no expenses, insurance is not an important factor in deciding which service to buy.

5. **Does the guarantee really protect you?** No identity theft service can guarantee that you won't become an identity theft victim. Guarantees are promises about what the service will do if you are victimized. They may provide for expense reimbursement and/or assistance resolving your problem. Some only promise to resolve problems resulting from a defect in the service. Read the guarantee carefully; it may not provide as much protection as you expect.

6. **What are the costs and terms?** Many identity theft services offer "free trials," during which you can test some of the features, but unless you have an identity theft problem immediately, you can't fully assess the service during the trial period. Pay attention to the terms of the trial offer; usually consumers must cancel before it ends to avoid charges. Some services charge month-to-month, others require payment upfront for a year or offer pre-payment options that are less expensive than paying month-to-month. Not all will provide a pro-rated refund if you decide to cancel before the term you paid for is up, however. Read the terms and conditions carefully to understand the cancellation policy.