Consumer Federation of America

Best Practices for Identity Theft Services: How Are Services Measuring Up?

April 18, 2012

Background

In March 2009 Consumer Federation of America released a report, *To Catch a Thief: Are Identity Theft Services Worth the Cost?*[1] The report, which was based on examining the websites and compiling information from other sources about 16 companies that provide identity theft services, assessed the claims that these services make, described practices that might be unfair or deceptive, provided consumers with information about how to shop for these services and the free or low cost options that are also available to them, and recommended public policy measures to address the problems that CFA found. Among those problems were overly broad claims about the ability to protect customers from identity theft and confusing, unclear and ambiguous descriptions of the services provided.

One of the report's recommendations was that the identity theft industry should develop best practices to encourage providing clear, accurate and complete information about what identity theft services do and to discourage unfair and deceptive practices. After CFA released the report, several identity theft service providers came forward to express similar concerns and offered to work with CFA on best practices. In October 2009 CFA brought company representatives and consumer advocates together to form CFA's Identity Theft Service Best Practices Working Group[2], and in March 2011 CFA released its *Best Practices for Identity Theft Services*.[3] In September 2011, CFA launched a new website, www.IDTheftInfo.org, to highlight the best practices and provide other resources about identity theft.

Now that the best practices have been out for a year, CFA decided that it was time to see how identity theft service providers are measuring up to them. The best practices are voluntary; there is no trade association that requires identity theft service providers to adhere to these best practices, nor does CFA provide any "seal of approval" or certification program. CFA strongly encourages all identity theft service providers to implement the best practices to help consumers understand exactly what they offer and under what terms. Having now examined identity theft services' websites through the lens of the best practices, CFA makes recommendations in this report for improving how key information is provided to consumers.

How CFA chose identity theft services to review

---

[1] www.consumerfed.org/elements/www.consumerfed.org/file/To%20Catch%20a%20Thief,%20March%2009.pdf

[2] For working group members who agreed to be publicly listed go to www.idtheftinfo.org/index.php?option=com_content&view=article&id=2&Itemid=2

[3] www.consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf. The Rose Foundation provided support for the *To Catch a Thief* report and the best practices project.

The best practices are aimed at for-profit providers of identity theft services. There are a wide range of services in the marketplace, from those that mainly monitor consumers' credit reports to services that monitor more broadly, looking for consumers' information in commercial and public databases and sometimes on the Internet where it may be fraudulently offered for sale. These services alert consumers about signs of possible identity theft. Some also provide anti-spyware software and other privacy protection tools. The benefits of membership often include access to one's credit reports, and increasingly to educational credit scores. Most services offer assistance if customers become identity theft victims. This fraud assistance usually consists of providing advice and counseling, but some services act on behalf of consumers to resolve their identity theft problems; in some cases that is the main feature of the service. Insurance, which typically covers out of pocket expenses for resolving identity theft and limited legal assistance, is also a common feature.

CFA searched online using the key words id theft protection, id theft service, and id theft assistance to find services that pop up frequently. Identity theft service providers that participated in CFA's best practices working group are also included in the study (except for Identity Theft 911, which individuals can't buy directly; see www.idt911.com). The services featured in this report are not the only ones in the marketplace, but they represent a good sample. Some identity theft service providers sell multiple services; in that case, CFA looked at the most comprehensive service they offer on their websites. All of the services that CFA reviewed can be purchased by individuals directly from the websites. In some cases, the services are offered by banks, insurance companies, or other entities that sell them in partnership with identity theft service providers. The best practices call on identity theft service providers to ensure that business partners and contractors follow the relevant best practices. Many identity theft service providers also sell their services to businesses, agencies and organizations that provide the services free to their customers, members or employees as a benefit or because of a data breach. Anyone who is shopping for identity theft services can use the best practices as a guide to help them choose services that follow good practices.

What CFA looked for and what it didn't

CFA looked at websites for identity theft services to see whether the information they provided met certain key elements of its best practices. As in the original study, CFA did not actually buy or test the services. And unlike the annual ratings of identity theft services conducted by Javelin Strategy & Research,[4] CFA did not attempt to determine which companies offer the most comprehensive services.

Some of CFA's best practices do not lend themselves to analysis by studying websites. For example, it wasn't possible for CFA to determine whether identity theft service providers have effective mechanisms for handling complaints, use reasonable and appropriate safeguards for personal information, or only obtain powers of attorney as needed and only use them for the stated purposes. Also, while the best practices encourage identity theft services to provide educational information to consumers, and many do so on the public sections of their websites, this information may be provided in

[4] Seehttps://www.javelinstrategy.com/news/1265/222/Rating-the-Products-that-Protect-Identities-in-a-Social-Mobile-and-Cyber-Age/d,pressRoomDetail .

welcome packets sent to members, in member-only sections of websites, in subscriber newsletters, and in other ways that could not be assessed in this study.

When it comes to privacy, the best practices set a high bar. CFA recognized that certain aspects of the privacy provisions, such obtaining opt-in consent to share individuals' personal information with third parties for marketing and giving individuals choice as to whether material changes to privacy policies will apply to personal information that has already been collected about them, may not be the standard practice for identity theft service providers and other companies at this point. In general, CFA found that while changes in privacy policies are posted on companies' websites, individuals aren't usually offered a choice as to whether those changes will apply to previously collected personal information (though some privacy policies state that if the company is sold, previously collected personal information won't be subject to any subsequent change in the privacy policies). As for sharing personal information with third parties for marketing purposes, the identity theft services that CFA looked at either don't engage in such sharing or, if they do, they give individuals the option to opt-out rather than asking them to opt-in.

Since individuals must rely on services' privacy policies to understand how their personal information is handled, CFA focused on the accessibility and clarity of those policies. Privacy practices continue to evolve. Recently both the White House and the Federal Trade Commission (FTC) issued reports citing the need for stronger privacy protection and recommending principles that businesses should adopt.[5] For instance, the FTC suggested that companies should obtain affirmative express consent before using consumer data in a "materially different manner than claimed when the data was collected."[6]

The best practices included in the study and the short descriptors that CFA used for them are shown below. Some of the best practices have been combined where they were closely related. The full set of the best practices, with more detailed explanations for each one, is appended to this report.

Don't misrepresent protection

Best Practice 1.1 Identity theft service providers should not misrepresent their ability to protect consumers from identity theft.

Provide clear information about how they protect/help consumers

Best Practice 1.2 Identity theft service providers should provide clear, accurate, and complete information about how they protect consumers and/or help them recover.

Best Practice 2.1 Identity theft service providers should make information about the features of their programs easily available to consumers before they enroll.

[5] *Consumer Data Privacy in a Networked World*, White House, February 2012, www.whitehouse.gov/sites/default/files/privacy-final.pdf; *Protecting Consumer Privacy in an Era of Rapid Change*, Federal Trade Commission, March 2012 http://ftc.gov/os/2012/03/120326privacyreport.pdf.
[6] See FTC report, id at page 60.

Best Practice 2.2 Identity theft service providers should clearly explain how the features of their programs may help consumers. This information should be made easily available to consumers before they enroll.

Best Practice 2.3 Identity theft service providers that alert customers about possible fraudulent use of their personal information should make information about how the alerts work and what the options are for receiving them easily available to consumers before they enroll.

Take care with statistics

Best Practice 1.3 Identity theft service providers should be careful when referring to statistics in promoting their services.

Don't misrepresent risk or harm of id theft

Best Practice 1.5 Identity theft service providers should not misrepresent the risk of identity theft or the harm it causes.

Provide basic company information

Best Practice 1.6. Identity theft service providers should make basic information about their companies and how to reach them easily accessible to consumers.

Cleary disclose refund/cancelation policy

Best Practice 1.7 Identity theft service providers should clearly disclose their cancelation and refund policies.

Provide clear privacy policy

Best Practice 1.9 Identity theft service providers should have clear, transparent privacy policies and make them easily available.

Provide clear, complete cost information

Best Practice 2.4 Identity theft service providers should provide clear and complete information about the cost of their programs to consumers before they enroll.

Don't request consumers' free credit reports

Best Practice 2.6 Identity theft service providers should not request customers' free annual credit reports in order to provide them with credit reports as a feature of their programs.

Clearly describe fraud assistance

Best Practice 3.1 Identity theft service providers that provide fraud assistance to identity theft victims should make thorough and accurate descriptions of exactly what that assistance entails, and any limitations or exclusions, easily available to consumers before they enroll.

Best Practice 3.2 Identity theft service providers should not misrepresent, directly or by implication, the fraud assistance they provide.

Clearly describe insurance/guarantees

Best Practice 3.3 Identity theft service providers that offer insurance as a benefit of their programs should make thorough and accurate information about what the coverage provides, under what circumstances, and any limitations and exclusions, easily available to consumers before they enroll.

Best Practice 3.4 Identity theft service providers that offer guarantees should make thorough and accurate information about what their guarantees provide, under what circumstances, and any limitations and exclusions, easily available to consumers before they enroll.

Best Practice 3.5 Identity theft service providers should not misrepresent, directly or by implication, the benefits of insurance or guarantees that they offer.

A note on the methodology

CFA began this project in late 2011 and re-reviewed all of the websites in March and April 2012, updating the findings as needed. The project was led by Susan Grant, CFA Director of Consumer Protection. She was assisted by Sean Naron, Administrative and Advocacy Associate at CFA, and Peggy Haney Ingalls, a retired financial service company executive who volunteered her time to help with the project. It is possible that changes have been made to identity theft service websites since CFA last looked at them. This study is intended to encourage companies to implement the best practices, and CFA's findings are not meant to be used as endorsements for any particular company or service.

An overview of what CFA found

In general, CFA found that the majority of the identity theft service websites met most of the best practices fairly well, though none received a perfect score. There are some overall concerns:

- **Some of the hype goes over the line.**

CFA expected that identity theft services would claim to be the most comprehensive, provide the best protection, and engage in other kinds of "puffery." But statements that services could "stop fraud before it starts," "stop identity theft in its tracks" or "prevent identity theft" seem to go over the line. Features such as anti-spyware software that a few services offer may in fact stop some attempts to steal consumers' personal information. But for the most part, identity theft services can't prevent identity theft – they can only alert customers when there are indications that their personal information may have been stolen. And they can't necessarily stop the stolen information from being used. If an identity theft service detects that a consumer's credit card number is being offered for sale on a rogue Internet site, the account number can be changed to prevent fraudulent use of it, if that hasn't already occurred. But it's not clear how much useful information about fraud is gleaned from Internet monitoring. Furthermore, if an Internet scan reveals that someone's Social Security number has been stolen, there is not much that can be done to stop it from being used, short of getting a new Social Security number, an

extreme measure that is usually not recommended because so much of one's legitimate identity is tied to that number. As for other types of monitoring, what they detect is the use of stolen information, at which point it's a matter of stopping the use from continuing if possible. Plus monitoring is only as good as the databases that are monitored, and it's not foolproof – some id theft may go undetected. CFA agrees with the advice offered in the press release for Javelin Strategy & Research's most recent identity theft service ratings: "Promote value, not hype," James Van Dyke, President and Founder of Javelin advises. "Don't aggressively market to consumers and don't lure them with promises of free credit reports that aren't really free or Internet scanning, which varies according to the quality of the database used."[7]

CFA recommendation: Identity theft services must avoid statements that overpromise how they can protect consumers.

- **There is some sloppy use of statistics.**

Statistics about the number of identity theft victims, the rate of identity theft, and the amount of time it takes to resolve identity theft problems are frequently used as marketing tools. CFA found that in most cases the sources of statistics were attributed, as the best practices call for. But the dates for statistics weren't always provided, and when they were, sometimes the statistics were old, so they weren't relevant if used to describe the current identity theft situation. CFA also found that complaint statistics were sometimes used to indicate the incidence rate of identity theft, which the best practices say not to do because complaint data are not representative of the population as a whole. In addition, sometimes identity theft services claimed to be "#1" or "top-ranked" without providing the source for the rating and/or the date on which it was bestowed.

CFA recommendation: Statistics used to describe identity theft should be the most recent available. Sources and dates should always be provided for statistics, and care should be taken to use complaint statistics properly.

- **Information about the features that services offer and how they work could be improved.**

CFA was impressed by how some identity theft services present information about the features they offer and how they work. On some websites, detailed information is provided on the home page or there are prominent tabs that lead consumers to it. Sometimes there are links from the features listed on the main product page to pop-ups, drop-down menus, expanded boxes, or other pages that provide more details. Frequently Asked Questions (FAQs) are often used to provide more details. In some cases key information about the features is only found in the terms of service or in membership agreements, which consumers might not read (even if they're asked to check a box indicating that they have). Sometimes CFA could not find certain details, such as the options consumers have for how to receive monitoring alerts, anywhere. Consumers shouldn't have to hunt through many different sections of identity theft services' websites to understand the features they offer. FAQ sections can be useful, but

[7] See https://www.javelinstrategy.com/news/1265/222/Rating-the-Products-that-Protect-Identities-in-a-Social-Mobile-and-Cyber-Age/d,pressRoomDetail.

neither they nor the terms of service should be the only places where consumers can find the details about how the features work. Now that credit scores are becoming a more common feature, it's important to explain that the educational scores that are provided are not the same as the scores that lenders use, though they are useful to help consumers understand why the information in their credit reports matters.

CFA recommendation: Critical details of services should be provided where they are first listed or in prominent links. All services must be clearly explained.

- **Refund and cancelation policies aren't always adequately disclosed; on disclosing the cost, services did better.**

Some identity theft services did a good job of providing information about their refund and cancelation policies; for example, by providing a clearly labeled link at the bottom of every web page. But in many cases CFA had difficulty finding that information. Sometimes it was only in the FAQs, the terms of service, or the enrollment pages. CFA also found that in some cases the policies were unclear. Regarding the cost of services, this information was usually clearly disclosed before consumers get to the page where they are asked for their information to enroll, as called for in the best practices. But in one case CFA couldn't find any information about what the cost would be after the free trial that was offered ended.

CFA recommendation: Refund and cancelation policies should be clear and easy to find, and all costs must be provided before the page where consumers sign up for the service.

- **In many cases the assistance provided to id theft victims still isn't clearly described.**

In its first study CFA found that the extent of the fraud assistance that identity theft services provide often wasn't clear. That continues to be a problem. Some identity theft services act on behalf of customers if they become victims – contacting creditors, law enforcement agencies, and others as needed, filing the paperwork, and doing whatever else may be required. Most services don't take an active role in resolving customers' identity theft problems, however. They typically provide victims with instructions about the steps they need to take, supply forms they may need to fill out, answer their questions, and provide moral support. With vague descriptions such as "a trained specialist will guide you through the process of recovering your credit and good name" or "24/7 access to helpful identity theft specialists," it's hard to tell exactly what services do for victims. Furthermore, details of the fraud assistance are sometimes only found in the terms of service or insurance policy.

CFA recommendation: Information about exactly what services do to help victims should be clear, straightforward, and easy to find.

- **Details about insurance are much easier to find.**

CFA believes that identity theft insurance is of little value, since it usually only provides reimbursement for out-of-pocket expense that for most victims will be minimal, and legal assistance that most will not need. Insurance is frequently touted as a feature of identity theft services, however, so it's important for

consumers to know exactly what it covers and what it doesn't. In CFA's first study, it was difficult to find the insurance details. This time, most of the websites that CFA looked at provided easy-to-find links to detailed insurance benefit summaries. But sometimes CFA had to hunt for the details, and some services didn't provide them at all. If the insurance information is only provided to consumers after they've enrolled, it's too late for them to compare coverage. It's also important for consumers to be able to tell upfront if the insurance covers pre-existing id theft and under what circumstances.

CFA recommendation: A detailed summary of the insurance should be provided via a link from wherever it's mentioned.

- **The most frequent complaint that CFA found about identity theft services concerns something not covered in the best practices – free trial offers.**

Many identity theft services offer the opportunity to try them for free, typically for a week or a month, after which consumers will be charged if they don't notify the company that they want to cancel. When CFA searched for complaints about identity theft services online on websites such as ripoffreports.com, they weren't about quality of the services themselves. That's not surprising, since the real test of these services is how well their alert systems and fraud assistance work when consumers become identity theft victims, and many will never experience that situation.

What CFA found instead were complaints about free trial offers. Often consumers said that they didn't realize that they had to cancel in order to avoid being charged at the end of the free trial period. In some cases they complained that they tried to cancel but could never get through to the company. And in some instances consumers asserted that they never agreed to try the service in the first place. This is not a problem exclusively with identity theft services; free trials are offered for many different kinds of services, and they are a common source of complaints. The terms aren't always made clear, and consumers aren't reminded when the trial periods are about to end. In many cases, free trials are offered in what's called "upselling" – a company that a consumer buys something from offers a free trial in something else, either a service of its own or that of an affiliate or marketing partner. Sometimes companies share customers' credit card or bank account information with other companies. This is especially troublesome, because consumers may not realize that companies they didn't give their account information to directly already have it and will use it to charge them when the trial period ends.

CFA recommends that companies should:

- ***Not share consumers' financial account numbers with affiliates or other companies for marketing purposes;***
- ***Provide consumers with 48 hours notice that a free trail is ending, along with information about how to cancel if they wish and the terms of the contract going forward if they want to continue using the service;***
- ***Provide quick and easy means of cancelation – no endless busy signals, no multiple hoops to jump through.***

How CFA did the scores

CFA uses these symbols to indicate how well identity theft services measured up to the best practices:

 Thumbs up means that it meets the best practice well; CFA might have a minor suggestion for improvement, but overall it does a good job.

 The hammer and nail means that it's pretty good but there is at least one substantive problem that needs to be fixed in order to attain the thumbs up score.

 Thumbs down means that it does a very poor job of meeting the best practice.

N/A means the best practice is not applicable; for instance, when no statistics are used on the website.

The charts that follow show how the identity theft services whose websites CFA examined measured up to the selected best practices. Explanations are provided for some of the scores.

This type of scoring is always difficult because it is somewhat subjective. In evaluating the websites, CFA looked at them from the consumer perspective: What are the most important things that consumers who are considering identity theft services need to know, and how good a job does the website do in providing that information in a clear, accurate, and accessible manner?

The best practices don't prescribe exactly how information should be presented, so the critiques and suggestions that CFA makes are intended to help identity theft service providers and their sales partners think about improvements they can make to fulfill the goals of the best practices.

Citi® Identity Monitor® https://creditcards.citi.com/services/citi-identity-monitor/?=f

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		We only found this on the enrollment page. We think this important information should also be provided before consumers get to that point.
Provide clear privacy policy		See note #2
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		It's not clear if the personnel at Citi Identity Theft Solutions only provide advice or if they contact creditors and others on your behalf.
Clearly describe insurance/guarantees		You can click on the policy to see the details of coverage depending on your state.

1. On the initial page for Citi Identity Monitor there is a brief description of the Key Services, under which it says Enroll Now. Clicking on this does not take you to the enrollment page, but rather takes you to a page with details about the service and links to additional information. We suggest that instead of Enroll Now, this link should be labeled something like Get More Details, How it Works, or Product Specs. There could also be links or pop-ups with more information right from the Key Services listed. We especially liked The Plain Language Box that spells out some of the details, but we could only find a link to that from the page that you fill out to enroll in the service. The information about the credit monitoring doesn't make its limitations in detecting id theft clear, and the information about the credit scores that are provided should make it clearer that they're not the same scores that lenders will use.

2. Clicking on Privacy Policy at the bottom of the web pages brings you Citi's website privacy policy. You must scroll down pretty far to see a reference to a separate Privacy Notice for Citi customers. This appears in a paragraph with no separate or bolded heading. The link from this reference brings you to the privacy policy that covers all of Citi's products and services. This link should be more prominently and clearly presented. For example, when consumers click on Privacy Policy they could be presented with two options: online privacy policy and product/service privacy policy. There is a question about privacy in the identity service FAQs, and the answer specifically refers to the identity theft product. This explanation is better than the general product/service privacy policy. It says that the actual Privacy Notice will be provided to you after you've enrolled, however. And we're not sure how many people would look for information about the privacy policy in the FAQs, especially since there is a link labeled Privacy Policy on the bottom of every page on the website.

Debix AllClear ID Pro www.allclearid.com

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		We like the fact that here are links from the features to more details about them.
Take care with statistics		Suggestion: the date should be provided for the Best in Resolution rating by Javelin Strategy & Research and for the Stevie Awards.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		See note #1
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		
Clearly describe insurance/guarantees		Suggestion: There is a link from the Protection Plans page but the type size could be larger. A link from the Pro page would also be helpful.

1. When you go to the section of the website for ID Pro, the fee-based service (there is also a less comprehensive free service) there is a link to FAQs, one of which explains how the 30-day free trial works and your ability to cancel at the end without being charged. But there wasn't any information there about cancelation if you wish to do so later. We found information about cancelation and refunds in the End User Services Agreement when we clicked on Terms. This information should be more easily available from the ID Pro section, and it should be provided in clear, non-legal language.

Equifax Complete™ Premier Plan www.equifax.com/premier

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics		
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		
Provide clear privacy policy		We like how clicking on Privacy Policy brings you links to the privacy policies for the various categories of products and services Equifax offers (id theft comes under Equifax Personal Products).
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		If you become a victim, you have access to an identity theft specialist, but we couldn't find information about what that person does for you.
Clearly describe insurance/guarantees		There are no details about what the "Up to $1 Million ID Theft Insurance" covers and what it doesn't, nor is any benefit summary provided.

1. Product Specs provides an overview of the features. But the video in How it Works doesn't really shed much further light. On the bottom of the main product page there is a link for important product disclosures. This takes you to Things You Should Know, which provides a bit more information about some of the features. In Frequently Asked Questions on the left there is a list of topics, some related to this product and some not. More information about some of the features is here – for instance, your options for receiving alerts. It would be a lot easier for consumers to get the details about the features if they were included in the Product Specs or if links were provided from there.

Experian ProtectMyID® Identity Theft Protection www.protectmyid.com

Don't misrepresent protection		We're giving phrases such as "Stop Identity Theft in its Tracks" the hammer and nail because we feel that they overpromise what the service can do.
Provide clear information about how they protect/help consumers		See note#1
Take care with statistics		Suggestion: In Our Product, FTC complaint statistics should not be used to describe the number of id theft victims a year.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		This information is only found in the FAQs.
Provide clear privacy policy		The privacy policy is easy to find and fairly clear, though the language could be plainer.
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		See note #2
Clearly describe insurance/guarantees		We like the fact that there is a link to the details of the insurance right from the home page.

1. On the home page, where some of the main features of the service are listed, one of the items is Medical Defense. But clicking on Learn more simply brings you to some general information about medical identity theft. We couldn't find any specific feature for detecting medical identity theft.

2. In Our Product, under Resolve, the description of the fraud assistance is better than many others that we saw, but we're still not sure what phrases such as "help contact the proper authorities," "assist with paperwork" and "take other vital steps" mean. Do they look up numbers and addresses for you, and send you forms that you need to file? Or do they actually make the contacts and do the paperwork for you? We'd like to see more straightforward descriptions of what the assistance entails.

EZShield® Platinum www.ezshield.com

Don't misrepresent protection		Claims in About Us that the company will "anticipate all forms of identity-related fraud" and "help shield your complete identity, on all fronts, all the time" go too far in assuring consumers that all they are protected against all eventualities.
Provide clear information about how they protect/help consumers		We like how in What do we offer? you can click on each feature to get more details.
Take care with statistics		Suggestion: The statistics in What is Identity Theft? are attributed, but the dates are not and should be provided.
Don't misrepresent risk or harm of id theft		We think the statement in What is Identity Theft? that "Everyone should have some form of Identity Protection" goes too far.
Provide basic company information		
Cleary disclose refund/cancelation policy		Our Promise says that customers can request full refunds up to 30 days of ordering. But it's not clear if consumers can cancel after that and whether money they may have prepaid will be refunded.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		It's clear that the company actually acts on consumers' behalf to resolve id theft problems.
Clearly describe insurance/guarantees		See note#1

1. In describing its 100% Service Guarantee in Our Promise, the company pledges that its Resolution Specialists will keep on working until customers are completely satisfied that their identities have been restored. But in Service Descriptions it says that resolution services won't continue if the company concludes that that the problem will never be resolved. The Terms and Conditions also make clear that the company doesn't guarantee that it will be successful in assisting customers with id theft problems to their satisfaction. The guarantee in Our Promise should more clearly reflect the fact that the company will do all that it reasonably can to resolve your identity theft problems.

ID Analytics www.myidalerts.com

Don't misrepresent protection		We think the company's claims that its alerts "Stop identity fraud before it starts" go too far. But we appreciate the disclaimer in How it Works that not all types of identity theft will be detected.
Provide clear information about how they protect/help consumers		
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		We only found this information in the FAQs.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports	N/A	
Clearly describe fraud assistance		See note #1
Clearly describe insurance/guarantees		There is a link to the summary of benefits right from the reference to insurance in How it Works.

1. How it Works says "you'll receive expert identity theft restoration assistance if you need it." But the only other reference to fraud assistance we could find was in the answer to a question in the FAQs about the company's alerts: I applied for credit and never received an alert, why? The response says that if an unauthorized account has been opened in the customer's name, an experienced fraud resolution professional will assist in shutting it down, and "if the subscriber does experience identity fraud a comprehensive identity remediation services is provided." But the insurance only provides the typical cost reimbursement and limited legal assistance, and we couldn't find any details about "comprehensive identity theft remediation services" on the site, so we don't know what they entail.

Identity Guard® Total Protection℠ www.identityguard.com

Don't misrepresent protection		We think the statement on the home page, "you can rest assured that the entire spectrum of your private information is protected," goes too far.
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics		Suggestion: On the home page the "Best-in- Class" rating source, date and category should be provided. The information is on the Total Protection page but it's too small and faint to read.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		We like the fact that there is a link to the refund policy right on the bottom of every web page.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		See note #2
Clearly describe insurance/guarantees		

1. We think the company generally does a good job explaining the features of the service and how they work. You don't have to hunt around several different sections of the website to find the information. But while the service provides extensive monitoring, we couldn't find information about how the alerts are delivered except for the credit monitoring feature. On the Total Protection page, key features are listed on the right; the first four have links to more information, but Identity Monitoring and Address Monitoring don't. Also, there is no explanation that the credit score that is provided is an educational score, not the same score that lenders will use.

2. Customers who become identity theft victims have access to the Identity Theft Assistance Center (ITAC) but there are no details on the Identity Guard site about the help that it provides. There is a link that brings you to the ITAC home page, which is confusing because in addition to providing assistance to Identity Guard customers, ITAC provides free assistance to customers of certain financial services companies, and ITAC also offers its own fee-based id theft service. The ITAC website doesn't say anything about Identity Guard customers and the information about exactly what the fraud assistance entails is not as clear as it could be. We suggest that Identity Guard provide more information about the fraud assistance on its own website and that if customers will be directed to the ITAC site, they should land at a section that clearly describes the fraud assistance that will be provided.

IdentityHawk www.identityhawk.com

Don't misrepresent protection		See note #1
Provide clear information about how they protect/help consumers		
Take care with statistics		Suggestion: While the statistics are attributed, some of them are really old and need to be updated.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		We found this only in the Member Agreement, which is full of legal jargon. This information should be more prominently disclosed.
Provide clear privacy policy		
Provide clear, complete cost information		You can sign up for a free trial offer through the website, but we couldn't find anything that says how much it costs after that.
Don't request consumers' free credit reports		
Clearly describe fraud assistance		The company makes it pretty clear that it provides advice about what you need to do to resolve your identity theft problem.
Clearly describe insurance/guarantees		There is a link to the summary of benefits on the bottom of every web page.

1. This service says it can "Stop fraud before it starts" and also claims to alert you "before they [identity thieves] commit the act." We think these claims go too far. And it says that its Social Security Number Protection will help make sure "you're the only one using it" and that by alerting you to unauthorized uses of your SSN you can take action before damage is done. But no identity theft service can make sure that no one is using your SSN, and if it is being used fraudulently, the only thing you can do is place fraud alerts on your credit reports and vigilantly monitor them and other records so that you can quickly try to resolve any damage.

Identity WorldWide www.identityworldwide.com

Don't misrepresent protection		See note #1
Provide clear information about how they protect/help consumers		In addition to the concerns in #1 and the lack of insurance details, there is no explanation that the credit score you get is not the same as lenders use.
Take care with statistics		
Don't misrepresent risk or harm of id theft		See note #2
Provide basic company information		Suggestion: This information is only in Terms and Conditions. It would be helpful to have an About Us or Contact Us that provides this information
Cleary disclose refund/cancelation policy		This information Is only in the FAQs and Terms and Conditions. It should be more prominently disclosed.
Provide clear privacy policy		The privacy policy is clear, but while you can opt of marketing from the company, it doesn't look like you can opt out of your personal information being shared with 3rd parties for marketing purposes.
Provide clear, complete cost information		You have to go to the FAQs or click on Get Protected Now to see that after 3 months for $3 the cost is $14.99 per month.
Don't request consumers' free credit reports		
Clearly describe fraud assistance		Suggestion: It's clear that victims get a self-help kit and phone counseling; we don't think that should be described as "world-class help and support."
Clearly describe insurance/guarantees		No details about the insurance benefits were provided on the website.

1. The company claims that by scanning underground chat rooms, websites and blogs where Social Security numbers are fraudulently offered for sale, it can help you make sure your SSN stays out of the hands of thieves, hackers and criminals. But at that point your SSN has already been stolen, and there is no way that you can prevent it from being sold or used.

2. In the description of the credit and debit card monitoring on the home page, it says that your cards are at risk whenever you make a transaction online. That's not true, since most commercial websites use security features to protect that information. Also, in Member Benefits, is says that recovering your identity is an arduous process. But sometimes it's not hard at all; it depends entirely on the situation.

ID Theft Assist www.idtheftassist.com

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics		Suggestion: The answer to the FAQ about whether to buy the service should not use FTC complaint statistics to indicate the incidence rate of id theft.
Don't misrepresent risk or harm of id theft		
Provide basic company information		Suggestion: We only found the physical address in the privacy policy. It would be helpful to also provide this in About Us or Contact Us.
Cleary disclose refund/cancelation policy		
Provide clear privacy policy		This is one of the clearest privacy policies we saw.
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		It's very clear that this service acts to resolve consumers' problems if they become id theft victims.
Clearly describe insurance/guarantees	N/A	

1. We really like how the features are all described in one place. While the main focus on this service is on providing fraud assistance, credit monitoring is offered but we didn't see anything describing the options you have for receiving alerts. You also get 24/7 access to your credit report and credit score, but we're not sure if it's a combined three-bureau report or from one bureau, and if it's the latter, which one. And there is no explanation that the score you receive isn't the one that lenders will use.

ID Watchdog Plus www.idwatchdog.com

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics		Suggestion: Many of the statistics on the website need to be updated.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		See note #2
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		The fraud assistance is very clear, as is the fact that if you're already a victim you can buy remediation services without subscribing to the other services.
Clearly describe insurance/guarantees		The service does not offer insurance; it plainly explains its guarantee to clear up records that have been affected by id theft.

1. We really like how the features are presented and explained on the website. But while the company says that it monitors thousands of databases, it doesn't mention whether it monitors consumers' credit reports and if so, at which credit bureaus. This would be helpful for consumers to know. Also, we only found the information about how the alerts are delivered and consumers' options in that regard in the FAQs. This information would be useful to include in the monitoring description as well.

2. There is an FAQ that says how to contact the company to cancel, but it does not describe the refund and cancelation policy. That's in the Terms and Conditions. We'd like to see this important information more prominently disclosed.

Intelius IdentityProtect www.intelius.com/idprotect.html?trackit=265

Don't misrepresent protection		See note #1
Provide clear information about how they protect/help consumers		See note #2
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		Suggestion: The physical address is only found from the www.intelius.com home page. This should be easier to find from the id theft section.
Cleary disclose refund/cancelation policy		You can cancel anytime with no further obligation if you pay monthly, but there is no information about the policy if you prepay for a year and then cancel.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		There is an explanation on the main product page about your right to get your free annual credit reports.
Clearly describe fraud assistance		This is only in the FAQs. It sounds like they notify creditors, file police reports, and do other thing for you, but it needs to be more prominent and clearer.
Clearly describe insurance/guarantees		An FAQ about insurance provides a link to the benefit summary, but we'd like to see a link from where the insurance Is listed on the product page.

1. The testimonial we saw on 4/7/12 (click on FAQs, then Testimonials) was from a woman who, before subscribing to this service, lost money when her debit card information was stolen. She says that the services' features would have helped her and specifically mentions the credit monitoring. But monitoring her credit reports wouldn't have alerted her to money being taken from her bank account. We're concerned that this may give the wrong impression about how that feature helps consumers.

2. Public records monitoring is listed as a feature on the main product page, but the details of this and all the other features are only in the FAQs. There it says that public records monitoring is provided with the IdentityProtect Premier membership. We couldn't find anything about the Premier membership even on the enrollment page. Maybe it's an option you can choose after the free trial? We're not sure.

ITAC Sentinel Premium® www.itacsentinel.com

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		See note #2
Clearly describe insurance/guarantees		There are no details about the insurance on the website.

1. We like how you get the details of the features by clicking on Learn More. You don't have to hunt all over the website to find the information. But we couldn't see how the monitoring alerts are sent, and there is no explanation that the credit score you get is not the one that will be used by lenders.

2. From the Sentinel product information, it's not clear what the fraud assistance entails. The details are only provided in an FAQ from the ITAC homepage (www.identitytheftassistance.org) ITAC will contact creditors to resolve your id theft problems, but we confirmed that its focus is only on credit-related id theft. If your stolen information is used for employment, government benefits or other purposes, you may get advice but no direct assistance. This needs to be clearer here and in the Sentinel information.

LifeLock Ultimate www.lifelock.com

Don't misrepresent protection		The claim in Scanning for Identity Theft that Internet scanning helps "stop thieves before they have a chance to commit fraud" goes too far.
Provide clear information about how they protect/help consumers		Suggestion: The explanation that the credit score you receive is not the same as lenders will use should not be only in the Terms and Conditions.
Take care with statistics		Suggestion: Some of the statistics are old and should be updated.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		See note #1
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		See note #2
Clearly describe insurance/guarantees		See note #3

1. We only found the refund and cancellation policy on in the Terms and Conditions, and it was confusing. You can cancel at any time without further obligation. But what if you've prepaid? It says that if LifeLock cancels your membership "without cause" and you have prepaid, you will get a pro-rated refund, but there is nothing about whether you'll get pro-rated refund if you decide to cancel. The refund and cancellation policy should be clearer and more prominently disclosed.

2. In Understanding How LifeLock works, clicking on Responding to Identity Theft brings you to a confusing statement. It is clear that if you lose your wallet, the service will help you get the contents replaced, with noted exceptions. But it's not clear if the next statement, "We'll help you contact your financial institutions and complete the necessary paperwork you need to get your life back in order,"

pertains just to the lost wallet feature. There is more information about LlfeLock's products from Choosing the Right Level of Protection; by expanding Respond to Identity Theft you see an explanation that the resolution team works "directly with lenders and providers," but it's still not clear exactly what they do. The insurance policy covers, among other things, "The amount of reasonable and necessary expenses paid to investigators and other third-party business providers that are retained by LifeLock and involved in any services that are reasonably necessary, viewed in the context of LifeLock's business and Membership Programs, to restore your good name and identity, or to recover your Losses in accordance with any Membership Program." This still doesn't make the fraud assistance clear, and elsewhere in the policy it describes a number of things that you are expected to do yourself, such as notify the credit bureaus, law enforcement, and others. We'd like to see a clearer explanation, not just in the insurance, about exactly what LifeLock fraud assistance does for you.

3. The page about the $1 Million Service guarantee provides a link to the insurance details, but since the guarantee and insurance are two different things, it might be better to have a separate tab for the insurance (there is also a link to the Insurance details in the Terms and Conditions). LifeLock was previously criticized for not making the terms of its Service Guarantee prominent and clear. Now you can click on an overview of the Service Guarantee right from the home page. It says that the company will spend up to $1 million to help you recover "if you become a victim of identity theft because of some failure or defect in our service." We're not sure how a consumer would know or be able to prove that identity theft happened because LifeLock didn't do something it promised to do, especially since no service, even if it works properly, can detect or prevent all id theft. It appears that customers are covered by the insurance even if they're not eligible for the Service Guarantee, but this a bit confusing.

Merchants Information Solutions SmartIdentity Platinum https://mcc.merchantsinfo.com/identity-theft-solutions.aspx

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		We only found this information in the Terms and Conditions. This important information should be more prominently disclosed.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		It's very clear that the service will act on your behalf to resolve your identity theft problems.
Clearly describe insurance/guarantees		There is an overview of the insurance when you click on Expense Reimbursement, but the details are in Terms and Conditions. There should be a link to that from the overview.

Privacy Guard http://www.privacyguard.com/content/identity-theft-protection.html

Don't misrepresent protection		See note #1
Provide clear information about how they protect/help consumers		Suggestion: Maybe we missed it, but we couldn't see how the monitoring alerts are delivered. This information should be provided.
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		This is very clear, but it's only on the enrollment page. We'd like to see this important information disclosed more prominently.
Provide clear privacy policy		
Provide clear, complete cost information		We only found the cost after the $1 one month trial on the enrollment page. The best practices call for cost to be disclosed before that.
Don't request consumers' free credit reports		
Clearly describe fraud assistance		See note #2
Clearly describe insurance/guarantees		

1. The company says its Social Security Monitoring will help you "prevent it [your SSN] from being used maliciously" and "take proactive measures before a thief has a chance to misuse it." But while you can put a fraud alert on your credit reports and vigilantly monitor your accounts for signs of fraud, there is no way you can absolutely prevent your SSN from being used once an identity thief has it.

2. This statement in How PrivacyGuard Helps You Recover (from Identity Theft Protection) is typical of the fraud assistance descriptions we found on many sites: "PrivacyGuard's extensive team of fraud recovery professionals will help you every step of the way in recovering your identity. This includes helping you contact creditors, filing paperwork and streamlining the credit dispute process." We're just

not sure what this means. Do they tell you how to contact creditors, or do they do that for you? Do they contact anyone else that may be necessary? Do the file the paperwork for you? Do they keep at it until your problems are resolved? We'd like to see fraud assistance described more clearly.

TransUnion zendough™ www.zendough.com

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		Suggestion: This information is only in the Product Agreement. It should be easier to find.
Cleary disclose refund/cancelation policy		This is only in the Product Agreement. While it's clear that you can cancel before the 7-day trial period ends, it's not clear what the refund and cancellation policy is after that.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		It is not clear exactly what the ID Recovery Assistance actually does.
Clearly describe insurance/guarantees		The Product Agreement provides a link to the insurance details but there should also be a link from the brief insurance description in My Identity.

1. My Identity, My Credit, and My Alerts provide some information about the features, but we found some details lacking. For instance, in My Identity, it says that Zendough "regularly reviews your risk and alerts you to any critical changes," but it's not clear what "regularly" means. It is not until you read the Product Agreement, a long document full of legal jargon, that you see that the credit monitoring includes all three major credit bureaus. The information about the credit scores you receive does not make clear that it is not the same score that lenders use. And we only found that the alerts are sent by email in the privacy policy, which is not a likely place for consumers to look for that information.

TrustedID® IDEssentials™ www.trustedid.com

Don't misrepresent protection		We think that the company's claims that this product will "help stop identity theft before it happens" go too far. Also see note #1
Provide clear information about how they protect/help consumers		See note #1
Take care with statistics		In How Identity Theft Affects You there are some statistics with an asterisk but we don't know what it corresponds with and could find no attribution.
Don't misrepresent risk or harm of id theft		Suggestion: In How Identity Theft Affects You it says that dealing with id theft is never easy. This is an overstatement and should be changed.
Provide basic company information		
Cleary disclose refund/cancelation policy		This information is only in the in the FAQs. It should be more prominently disclosed.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		See note #2
Clearly describe fraud assistance		See note #3
Clearly describe insurance/guarantees		There is a link to the Service Warranty right from the home page.

1. We like the way the features have links to more details, but we found some information lacking or potentially misleading. The Medical Benefits Protection helps you review your insurance statements to spot unauthorized medical services. But this doesn't "ensure that you and your family are the only ones being treated with your medical benefits." The explanation that online access to your credit reports will enable you to "make sure that no one has been stealing your identity to commit fraud" is troublesome because not all types of identity theft show up on credit reports, and when something does show up it means your identity has already been stolen. In explaining the credit score feature, it says that you will "see the scores that lenders look at when deciding to give you a loan or line of credit," but they are not

the same score that lenders will use. Plus, we could not find information about how the monitoring alerts are sent.

2. From the Terms of Service, it sounds like the company requests your free annual credit reports, charging you for something that you can do yourself at no cost and preventing you from requesting your free credit reports for the next 12 months.

3. The details of the fraud assistance are only in the Service Warranty. While there is a prominent link to the Service Warranty from the home page, it may not be clear from the brief description there, which talks about covering out of pocket expenses if you become a victim, that the Service Warranty is where you will find the information about what the “live, on-call protection specialists” mentioned in another part of the home page actually do for you.

Wells Fargo Enhanced Identity Protection
www.wellsfargo.com/insurance/id_credit_protection/idtheft?ref=WELLSROSPAG0066&eitp=WELLSCONFRM0008

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		
Take care with statistics	N/A	
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		We only found this information on the enrollment page. It should be more prominently disclosed earlier on.
Provide clear privacy policy		Suggestion: Clicking on Privacy Policy brings you to a list of policies; we assume that the Privacy Policy for Individuals applies, but it could be clearer. There could also be an FAQ about privacy with a link.
Provide clear, complete cost information		
Don't request consumers' free credit reports		
Clearly describe fraud assistance		See note #1
Clearly describe insurance/guarantees		No details about the insurance are provided.

1. We think this description of Support, " A dedicated specialist to work with you in restoring your identity, supporting you every step of the way and providing on-going assistance through the recovery process," is too vague.

Zander Insurance Group Identity Theft Protection www.zanderins.com/idtheft/idtheft.aspx

Don't misrepresent protection		
Provide clear information about how they protect/help consumers		
Take care with statistics		Some of the statistics are very old. And in the FAQs there are some statistics that aren't attributed and we're not sure when they are from.
Don't misrepresent risk or harm of id theft		
Provide basic company information		
Cleary disclose refund/cancelation policy		This is in the Services Contract. We'd like to see it disclosed right on the product page.
Provide clear privacy policy		
Provide clear, complete cost information		
Don't request consumers' free credit reports		There is a link right on the product page to help you request you free annual credit report.
Clearly describe fraud assistance		The description of fully managed recover is very clear.
Clearly describe insurance/guarantees		There is a link to the summary of insurance benefits right from the product page.

APPENDIX

Text of Consumer Federation of America Best Practices for Identity Theft Services[8]

SECTION 1. GENERAL GUIDELINES

1.1 Identity theft service providers should not misrepresent their ability to protect consumers from identity theft.

Identity theft service providers should only make representations in regard to protecting consumers from identity theft that are truthful and that they can adequately substantiate. It is misleading to represent or imply that identity theft services can absolutely prevent information about individuals from being stolen or fraudulently used. In promoting and selling their services, identity theft service providers should refrain from making broad claims that would lead consumers to believe that they can provide complete protection against all forms of identity theft, detect all instances of identity theft, or stop all attempts to commit identity theft. Identity theft service providers should be very careful when using descriptions such as "comprehensive," "complete protection" and the like. It is important to avoid implying that their services will absolutely prevent identity theft.

1.2 Identity theft service providers should provide clear, accurate and complete information about how they protect consumers and/or help them recover.

There is a wide range of identity theft services available in the market. Some offer monitoring services, others do not. Monitoring may be for certain types of information and not others. Some services offer assistance to fraud victims, others do not. The extent of fraud assistance and eligibility for it may vary. To help consumers choose the services that best fit their needs, identity theft service providers should provide clear, accurate and complete information about how they protect customers and/or help them recover. For further guidance about describing the features and costs of services and the fraud assistance provided, see Sections 2 and 3 of these best practices.

1.3 Identity theft service providers should be careful when referring to statistics in promoting their services.

[8] For the complete best practices document including the introduction, scope, and table of contents go to www.consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf.

Representations about survey or study results may be deceptive if the underlying survey or study was not conducted in a competent and scientifically valid manner. Even when a survey or study is carefully performed, it is important not to misrepresent the results. For example, if an identity theft service provider sent a survey to a randomly selected sample of 1,000 customers to ask if they were satisfied with the service and only 100 people answered the survey (with 70 of them saying "yes" and 30 saying "no"), it would be misleading to say that 70 percent of the customers were satisfied with the service.

Identity theft service providers should provide the source for any claims such as "the #1 identity theft service" or "the top-ranked service" and the date on which that ranking was issued. If identity theft service providers refer to their own "success" rates – for instance, in resolving customers' fraud problems – they should make clear how they define "success" and how they calculated the statistics in order to substantiate those claims.

When identity theft service providers use external statistics in promoting their services to describe the magnitude or impact of identity theft in general or of particular types of identity theft, they should provide the specific source of the information and the date that it was issued. This can be incorporated in the statement – for example, "According to a 2010 survey by…" The information could also be placed in a footnote, or disclosed in another conspicuous manner. It is helpful to provide a link to the source, if available.

While the ranking of identity theft relative to other types of complaints may be cited ("Identity theft was the top complaint received by X in 2010"), the number of complaints that agencies or organizations have received about identity theft should not be used to indicate the incidence rate of identity theft, nor should changes in the number of complaints be used to support a claim that identity theft is increasing or decreasing. Complaint data are not representative of the population as a whole. Changes over time in the number of complaints received may reflect changes in the percentage of identity theft victims who report their experience to the particular agency or organization rather than changes in the number of people experiencing identity theft.

1.4 Identity theft service providers should ensure that testimonials and endorsements they use to promote their services are not misleading.

Endorsements and testimonials that identity theft service providers use to promote their services must reflect the honest opinions or experiences of those who make them. If an endorsement or testimonial is from someone who is depicted as having used the service, that person must have been a customer at the time of the service provider's action to which the endorsement or testimonial refers.

If the results reported by a consumer's testimonial are not representative of what customers using the service will generally achieve in the circumstances described by that individual, the identity theft service provider should clearly and conspicuously disclose the results that customers should generally expect under the depicted circumstances. For instance, if the customer's testimonial says "They resolved my identity theft problems in less than 24 hours!," but the majority of identity theft problems take two weeks to resolve, the identity theft service provider should clearly note the typical time to resolve those problems. Testimonials and endorsements do not have an infinite shelf life; they should reflect the identity theft service provider's current services and methods of operation.

When an identity theft service provider uses an endorsement or testimonial that is attributed to an expert, that person should have expertise in the relevant subject matter. Endorsements or testimonials by organizations should be based on a process sufficient to ensure that they fairly reflect the collective judgment of the organization.

When there is a connection between the identity theft service provider and the person or organization making the endorsement or testimonial that might materially affect its weight or credibility (in other words, consumers would not reasonably expect that relationship), that connection should be clearly and conspicuously disclosed. For instance, if a customer who provides a testimonial for the service has been paid to do so, that would be something that consumers would not expect and that would likely affect the credibility of the testimonial. In that case, the fact of the payment should be disclosed.[9]

1.5 Identity theft service providers should not misrepresent the risk of identity theft or the harm it causes.

While identity theft is a serious problem, not everyone is or will become a victim, and the impact of various forms of identity theft varies widely. In promoting and selling their services, identity theft service providers should not misrepresent directly or by implication the risk of identity theft to consumers in general or to particular consumers, or the harm that consumers are likely to suffer as a result. For example, it would be a misrepresentation to state or imply that all consumers who have Social Security numbers are likely to become identity theft victims.

1.6 Identity theft service providers should make basic information about their companies and how to reach them easily accessible to consumers.

Consumers who are considering purchasing identity theft services should be able to find the information necessary to ask questions and check a service provider's complaint records. On

[9] See the Federal Trade Commission's Guides Concerning Use of Endorsements and Testimonials, CFR 16 § 255, http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=27e5bd89274ead18e368ffa4a09a7b7e&rgn=div5&view=text&node=16:1.0.1.2.22&idno=16. State laws and regulations may also apply.

their websites, identity theft service providers should make basic information about their companies easily accessible, such as:

- The incorporated company name and any DBAs;
- Product line names;
- The physical location of the service provider's headquarters;
- Whether the service provider is licensed, registered or bonded in particular states and how to contact the relevant agencies;
- Membership in the Better Business Bureau or any other type of accrediting organization and how to reach that organization;
- How to contact the service provider or product distributor directly for answers to pre-enrollment questions.

Advertisements and promotional materials should provide the Web address and a toll-free number, if there is one, through which consumers can obtain information about the company.

1.7 Identity theft service providers should clearly disclose their cancelation and refund policies.

Before consumers subscribe to identity theft services it is important for them to know whether and how they can cancel, whether and how they can obtain refunds, and under what circumstances. This information should be clearly disclosed on identity theft service providers' websites if the service is offered online, and in their contracts, and should be available from the representatives at their toll-free numbers, if they have them.

1.8 Identity theft service providers should provide effective mechanisms for handling complaints in order to provide the highest level of customer satisfaction.

Customers should be able to make complaints about identity theft services easily and get them resolved quickly. Information about how to contact the provider or a third party designated to handle complaints should be clearly disclosed on identity theft service providers' websites and in their contracts and should be available through their toll-free numbers, if they have them. Identity theft service providers should provide effective mechanisms for responding to customer complaints, including complaints about services provided by subcontractors. If identity theft service providers contract with third parties to handle their complaints, they should monitor them closely to identify and correct problems and enhance customer satisfaction. Identity theft service providers should take prompt and appropriate action when they are notified about complaints by consumer protection agencies, the Better Business Bureau, or other organizations.

1.9 Identity theft service providers should have clear, transparent privacy policies and make them easily available.

Identity theft service providers may collect a range of personal information from or about individuals, such as their addresses, phone numbers, email addresses, Social Security numbers, financial account numbers, and information about family members. This information may be used for a variety of purposes, including verifying individuals' identities, processing payments, providing monitoring and lost wallet services, helping to resolve fraud problems, and marketing products or services. Privacy is an important issue, especially since people who inquire about or enroll in identity theft services may have heightened concerns about the potential to become identity theft victims or may already be victims.

Identity theft service providers should have clear, transparent privacy policies that explain:

- What types of personal information they collect from or about individuals;
- How and with whom the information is shared and for what purposes;
- What options individuals have to limit the collection and/or use of their personal information and how to exercise those options;
- How the information is safeguarded in transmission, storage and disposal;
- How to contact customer service for questions regarding the privacy policy.

Privacy policies should be written in plain language and presented in a format that is concise and easy to read. Privacy policies should be conspicuously posted on identity theft service providers' websites[10] and should be provided to new customers in writing or electronically.[11] Customer service personnel should be trained to answer questions about the privacy policy.

[10] The description of "conspicuously post" under California law regarding privacy policies on commercial websites may be helpful, see. http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22575-22579. The California Office of Privacy Protection offers guidance for making privacy policies recognizable and readily accessible at www.privacy.ca.gov/res/docs/pdf/infosharingdisclos.pdf, page 12.

[11] Companies that are subject to the Gramm-Leach-Bliley Act (GLB) must provide consumers with written or electronic notice describing their privacy policies by the time of establishing customer relationships and annually thereafter. The Federal Trade Commission provides advice about complying with GLB at http://business.ftc.gov/documents/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act. If providing the initial description of the privacy policy by the time the customer relationship is established would substantially delay the transaction, it can be provided within a reasonable time after as long the consumer agrees. Under these best practices, identity theft service providers should follow similar procedures for the initial notice even if they are not covered by GLB.

Identity theft service providers should not collect more personal information from or about individuals than is needed for the purposes stated in their privacy policies and should only use the information for those purposes.

Identity theft service providers should provide individuals whose personal information they maintain with a minimum of 30 days notice prior to implementing any material changes to their privacy policies. Examples of a material change in this context include: collecting personal information that was not collected previously; using personal information in a way that it was not used previously; sharing personal information with a type of entity with which it was not previously shared; or placing new restrictions on individuals' choices regarding the collection, use or sharing of their personal information. For instance, it would be a material change to share an individual's personal information with third parties for marketing purposes if the privacy policy did not previously provide for that. Before material changes to privacy policies are applied to personal information that has already been collected, identity theft service providers should provide a clear and concise notice of all material changes directly and separately to each individual, which shall also contain an easy-to-use method for the individual to express his or her choice in that regard. Pre-checked acceptance should not be used. Notices should be sent by mail when recipients are not set up for online delivery.

1.10 Identity theft service providers should use reasonable and appropriate safeguards to protect individuals' personal information and should not misrepresent their security measures.

Identity theft service providers should establish, implement and maintain a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about individuals. When contracting with third parties for any aspect of their promotions or operations, identity theft service providers should require that they also use reasonable and appropriate safeguards to protect such personal information. Identity theft service providers should ensure that individuals whose personal information they maintain receive appropriate responses to security breaches.

Identity theft service providers should have written retention polices and keep individuals' personal information only as long as it is relevant and necessary according to those policies. Identity theft service providers should also adopt policies and procedures to safely dispose of such information when it is no longer needed.

Identity theft service providers should not misrepresent, directly or by implication, the manner or extent to which they maintain and protect the privacy, confidentiality, or security of personal information collected from or about individuals.

1.11 Identity theft service providers should use special care if they provide individuals' personal information for third-party marketing purposes or facilitate sales by third parties.

Since individuals who inquire about or enroll in identity theft services are concerned about becoming victims – and in some cases already are – they may be especially sensitive about personal information being provided to parties with which they have no relationship, for purposes unrelated to providing the identity theft services. Identity theft service providers should obtain individuals' express affirmative consent through an opt-in procedure before providing their personal information to third parties for marketing purposes. Because of the sensitivity and the risk of abuse, identity theft service providers should not provide individuals' financial account numbers or Social Security numbers to third parties for marketing purposes.

If identity theft service providers facilitate sales of goods or services by third parties through their websites or telemarketing operations, they should clearly disclose that those offers are from third parties and clearly present options to accept or decline them. For example, on an identity theft service provider's website, a button to decline a third party offer should be as prominent as a button to accept it. Consumers should be required to affirmatively accept offers from third parties through a click or step that clearly confirms their assent. Pre-checked acceptance should not be used to obtain individuals' consent to provide their personal information to third parties for marketing purposes or to obtain their acceptance for offers from third parties.

1.12 Identity theft service providers are encouraged to provide basic educational information to consumers about their rights in relation to identity theft and how to reduce the potential to become victims.

Identity theft service providers are in a unique position to help educate consumers about identity theft. On their websites and in other materials, as appropriate, identity theft service providers are encouraged to provide basic information, or links to information, about consumers' rights in relation to identity theft and how to reduce the potential to become victims. This may include but is not limited to:

- Information about consumers' rights to obtain free annual copies of their credit reports and a link to the central source for requesting their free annual reports.

- Information about how security freezes work, what their effect is, and how consumers can find more information about placing them on their credit files.
- Information about how fraud alerts work, what their effect is, and how consumers can place them on their credit files if they suspect that they are or may be about to become victims of fraud.
- Information about how active duty alerts work, what their effect is, and how consumers can place them.
- An explanation of the differences between fraud alerts and security freezes.
- Information about how consumers can remove themselves from marketing lists, protect their computers from hackers and spyware, guard against phishing, protect their Social Security numbers from unnecessary use, and safeguard their mail.
- Information about how consumers can get inaccurate information resulting from identity theft removed from their credit reports.

SECTION 2. INFORMATION ABOUT PROGRAMS

2.1 Identity theft service providers should make information about the features of their programs easily available to consumers before they enroll.

The features of identity theft programs vary from one identity theft service provider to another. Some providers offer multiple programs with different features. Information about the features of identity theft programs should be easily available to consumers before they enroll to enable them to compare programs and prices and determine if there are additional steps they may need to take to protect themselves.

For instance, if the program monitors customers' credit reports, the identity theft service provider should specify the credit reporting agency or agencies included. This would enable consumers to compare that program with other programs that feature credit monitoring. If consumers choose a program that does not include all of the credit reporting agencies, they might decide to take it upon themselves to check their reports at the credit reporting agencies that are not included. While it may not be practical, or wise, to specifically name other databases, records and websites that may be monitored, identity theft services providers should clearly describe the types of databases, records and websites that are included and state how frequently the monitoring is conducted.

When features of identity theft programs require Internet or email access or the capability to run certain computer programs, this fact should be clearly stated.

Identity theft service providers' advertisements and marketing materials should provide a toll-free number, if there is one, and a website where consumers can obtain full information about the features of their programs. On their websites, identity theft service providers should make detailed information about the features of their programs easy to find. This information could be provided in a layered manner, with links from the highlights to more details. Describing the assistance that will be provided to fraud victims is addressed in Section 3.

2.2 Identity theft service providers should clearly explain how the features of their programs may help consumers. This information should be made easily available to consumers before they enroll.

Some features that may be included in identity theft services are fairly straightforward and there is little potential for consumers to be confused about what to expect. A "lost wallet" feature that enables consumers to store information about their financial accounts with the identity theft service provider and get assistance with contacting their financial service providers in the event they lose their wallets is easy to understand. It may be more difficult, however, for consumers to understand the benefits and limitations of other features. For instance, since many consumers may not know what kind of identity theft problems credit monitoring or public record monitoring may help to detect, they could have unrealistic expectations in that regard.

To help consumers understand the benefits and limitations of their programs, identity theft service providers should clearly explain how the features can help them. For example, if credit monitoring is a feature, the identity theft service provider should explain the types of information that credit reports usually contain and that credit monitoring can provide early detection of new account fraud. This information should be made easily available to consumers before they enroll. Identity theft service providers should be careful not to overstate or misrepresent, directly or by implication, how the features of their programs may help consumers.

2.3 Identity theft service providers that alert customers about possible fraudulent use of their personal information should make information about how the alerts work and what the options are for receiving them easily available to consumers before they enroll.

There are many ways to alert consumers about possible fraudulent use of their personal information, including phone, mail, text, email, and other messaging technologies. Because consumers' technical capabilities and preferences vary, it is important for identity theft

service providers to make information about how alerts work and what the options are for receiving them easily available to consumers before they enroll.

2.4 Identity theft service providers should provide clear and complete information about the cost of their programs to consumers before they enroll.

It is crucial to provide clear and complete cost information for identity theft services before consumers are asked for any enrollment information. For example, on a website, this would be before consumers get to the page where they are asked to provide their names, addresses, and other information needed for enrollment. The cost information should be provided again at the point when consumers are asked to provide payment information.

Consumers are sometimes offered identity theft services at no charge as a benefit of employment, as the result of a data breach, or in similar circumstances. Before renewing the service at the customers' cost, identity theft service providers should provide clear and complete cost information and obtain customers' affirmative consent to renew.

2.5 Identity theft service providers should ensure that any statements they make about fraud alerts in connection with their programs are complete and accurate and do not mislead consumers, directly or by implication, about the protection that fraud alerts provide.

Fraud alerts can help prevent identity thieves from fraudulently using consumers' personal information to open new accounts when the consumers' credit reports are checked as part of the credit granting process. However, fraud alerts do not prevent all fraudulent use of consumers' personal information. Identity theft service providers should ensure that any references they make or explanations they provide about fraud alerts in connection with their programs are complete and accurate and refrain from making statements that would mislead consumers, directly or by implication, about the protection that fraud alerts provide.

2.6 Identity theft service providers should not request customers' free annual credit reports in order to provide them with credit reports as a feature of their programs.

Under federal law, consumers are entitled to request their credit reports free annually from each of the credit reporting agencies through an officially-designated centralized source. Many identity theft service providers furnish customers with their credit reports periodically as a feature of their programs by purchasing the reports from the credit reporting agencies. However, some identity theft service providers furnish customers with their credit reports by

requesting their free annual reports from the centralized source. This practice causes confusion and denies customers the ability to obtain their free annual reports themselves for a twelve month period. Identity theft service providers should not request customers' free annual credit reports in order to provide them with credit reports as a feature of their programs.

SECTION 3. FRAUD ASSISTANCE

3.1 Identity theft service providers that provide fraud assistance to identity theft victims should make thorough and accurate descriptions of exactly what that assistance entails, and any limitations or exclusions, easily available to consumers before they enroll.

Some identity theft services provide fraud assistance to identity theft victims, directly or through contracted services. Fraud assistance varies widely. In some cases, it consists of providing information about the steps that customers should take on their own to resolve their identity theft problems. The service may provide forms for customers to use, such as affidavits. Some identity theft service providers also offer one-on-one counseling to help guide customers through the process of resolving their identity theft problems. Others go further, actually contacting creditors, employers, law enforcement agencies, and others as needed on behalf of customers to help resolve their identity theft problems. Some identity theft service providers follow up with the entities that they contacted on behalf of their customers to ensure that the problems are resolved, while others do not. Legal representation may be provided to assist customers in actions taken to collect debts incurred by identity thieves, in criminal cases in which defendants have used the customers' identification, and/or in other circumstances arising from identity theft.

It should be easy for consumers to find thorough and accurate descriptions of exactly what the fraud assistance that is offered entails, and any limitations or exclusions, before they enroll in the service. In addition to the detailed information that appears in the terms of service, identity theft service providers should clearly and conspicuously disclose on their websites, and make available through the representatives at their toll-free numbers, if they have them, sufficient information about the fraud assistance they offer for consumers to make informed decisions.

That information should include whether identity theft service providers offer assistance with problems arising from identity theft that occurred before the date of enrollment; if so, under what circumstances; and whether there is an additional charge in that case.

3.2 Identity theft service providers should not misrepresent, directly or by implication, the fraud assistance they provide.

In promoting their services, identity theft services should avoid leading consumers to believe that the fraud assistance they provide is more extensive than it is. For instance, identity theft service providers should not misrepresent, directly or by implication, that they will resolve customers' identity theft problems if they do not actually contact creditors and others, as necessary, on their customers' behalf and follow up to ensure that the problems are resolved. If identity theft services providers help customers resolve their identity theft problems by providing advice about the steps that customers should take on their own, they should avoid misrepresenting the extent of that assistance by making clear whether they provide general information or if they provide one-on-one counseling to actively help guide them through that process.

3.3 Identity theft service providers that offer insurance as a benefit of their programs should make thorough and accurate information about what the coverage provides, under what circumstances, and any limitations and exclusions, easily available to consumers before they enroll.

Many identity theft services offer insurance as a benefit of their programs. Insurance policies are regulated by the states in which consumers reside. Identity theft service providers that offer insurance should abide by all relevant state laws and regulations.

Insurance policies vary widely in terms of the coverage they provide. They often reimburse customers for out-of-pocket expenses that they have incurred in resolving their identity theft problems, such as notary fees, postage, and telephone calls. In some cases they provide limited reimbursement for time that customers must take off from work to resolve their problems. Some cover the cost of legal representation, which usually requires the customer to obtain approval before hiring an attorney or to use an attorney retained by the insurer or the identity theft service provider. Often there are limitations and exclusions. For instance, an incident may not be covered if the fraud was committed by a family member, or unauthorized charges to a victim's credit card account may not be reimbursed under the policy. There may be notice and documentation requirements in order to make claims under the policies.

Identity theft service providers that offer insurance should make thorough and accurate information about what the insurance coverage provides, under what circumstances, and any limitations and exclusions, easily available to consumers before they enroll. In doing so, they should consider what consumers might expect would be covered and make clear if it is not – for

instance, that reimbursement is not provided for money that identity theft thieves have stolen from customers, if that is the case. If the insurance policy requires the consumer to pay a deductible, this should be clearly explained. It is also important to clearly describe how any legal assistance that is provided works. For instance, if prior approval is required, if the choice of attorney is not made by the consumer, and/or if legal representation is only provided for certain matters such as suit by creditors but not for criminal defense, this should be clearly spelled out.

In addition to the detailed information in the terms of service, identity theft service providers should clearly and conspicuously disclose on their websites, and make available through the representatives at their toll-free numbers, if they have them, sufficient information about the insurance they offer for consumers to make informed decisions. Identity theft services are also encouraged to provide a link on their websites to the actual insurance policy, if possible.

3.4 Identity theft service providers that offer guarantees should make thorough and accurate information about what their guarantees provide, under what circumstances, and any limitations and exclusions, easily available to consumers before they enroll.

Many identity theft services offer guarantees. In some cases guarantees are underwritten by insurance companies, in others they are provided directly by the identity theft service providers. Guarantees vary widely in terms of what they provide to consumers. Some offer the same type of benefits as described in 3.3, and there may also be similar limitations, exclusions, and documentation requirements. In some cases, the guarantees simply consist of a promise to take all steps necessary on behalf of customers to resolve their problems if they are identity theft victims.

Identity theft service providers that offer guarantees should make thorough and accurate information about what their guarantees provide, under what circumstances, and any limitations and exclusions, easily available to consumers before they enroll. In doing so, they should consider what consumers might expect would be covered and make clear what is not – for instance, that reimbursement is not provided for money that identity theft thieves have stolen from customers, if that is the case. In addition to the detailed information that appears in the terms of service, identity theft service providers should clearly and conspicuously disclose on their websites, and make available through the representatives at their toll-free numbers, if they have them, sufficient information about the guarantees they offer for consumers to make informed decisions.

3.5 Identity theft service providers should not misrepresent, directly or by implication, the benefits of insurance or guarantees that they offer.

In promoting their services, identity theft service providers should avoid leading consumers to believe that the insurance or guarantees they offer provide greater benefits than they do. For example, insurance policies and guarantees do not provide cash payouts to customers simply because they have become identity theft victims, but advertisements might lead consumers to believe that they do unless more information is provided.

3.6 Identity theft service providers should obtain powers of attorney only as needed to help their customers and use them only for the stated purpose.

Identity theft service providers sometimes need a document called a power of attorney in order to act on behalf of customers who request assistance. A power of attorney should be written in clear and simple language that describes the scope of the power given to the identity service provider, how long the power of attorney will last, and how to revoke it. A power of attorney should only be obtained when the need arises, and should be limited to the purpose of providing the assistance that the customer requested. The power of attorney should be terminated and destroyed as soon as it is no longer needed for the stated purpose, or upon receipt of a the customer's written or oral request to revoke it, or upon termination of the relationship with the customer.