

Consumer Federation of America
Best Practices for Identity Theft Services

March 10, 2011

Consumer Federation of America
Best Practices for Identity Theft Services

Table of Contents

Introduction	3
About Consumer Federation of America	4
Identity Theft Service Providers	4
Scope of the Best Practices	5
Section 1. General Guidelines	6
1.1 Not misrepresenting the ability to protect consumers from identity theft.	6
1.2 Providing information about protecting or helping consumers recover.	6
1.3 Referring to statistics in promoting identity theft services.	6
1.4 Ensuring that testimonials and endorsements are not misleading.	7
1.5 Not misrepresenting the risk of identity theft or the harm it causes.	8
1.6 Making basic information about companies easily accessible to consumers.	8
1.7 Clearly disclosing cancelation and refund policies.	9
1.8 Providing effective mechanisms for handling complaints.	9
1.9 Having privacy policies and making them easily available.	9
1.10 Using reasonable and appropriate safeguards to protect personal information.	11
1.11 Providing individuals' personal information to or facilitating sales by third-parties.	11

1.12 Providing basic educational information to consumers.	12
Section 2. Information about Programs	13
2.1 Making information about the features of programs easily available.	13
2.2 Clearly explaining how the features of programs may help consumers.	13
2.3 Providing information about how alerts about possible fraud work.	14
2.4 Providing information about the cost of their programs.	14
2.5 Ensuring that any statements about fraud alerts are complete and accurate.	15
2.6 Requesting customers' free annual credit reports.	15
Section 3. Fraud Assistance	16
3.1 Describing what fraud assistance provided entails.	16
3.2 Not misrepresenting the fraud assistance provided.	16
3.3 Providing information about insurance.	17
3.4 Providing information about guarantees.	18
3.5 Not misrepresenting the benefits of insurance or guarantees.	18
3.6 Obtaining and using powers of attorney.	19

Consumer Federation of America

Best Practices for Identity Theft Services

Introduction

In March 2009, Consumer Federation of America released a report¹ about identity theft services based on examining the websites of 16 identity theft service providers. Additionally, news reports, lawsuits, and other sources of information were reviewed in compiling the report. The purpose of CFA's study, funded by a grant from the Rose Foundation, was to assess the claims these services make, describe unfair and deceptive practices in the promotion and operation of these services, inform consumers about their legal rights and the free or low-cost options available to help them with identity theft, advise consumers about how to shop for identity theft services, and recommend public policy measures to prevent unfair and deceptive practices in the industry. CFA found that the descriptions of how these services help consumers were often confusing, unclear, and ambiguous, and that the services did not always offer the protection that consumers were led to expect.

One of the recommendations in the report was that the identity theft industry should develop best practices to encourage companies to provide clear, complete information about their services and discourage unfair and deceptive practices. There is no industry trade association, but in discussions with individual identity theft service providers CFA learned that they shared the concerns raised in the report and were interested in working together to improve industry practices. In October 2009, CFA convened a meeting with representatives of identity theft service providers, nonprofit consumer organizations, and government consumer protection agencies to discuss the problems highlighted in the report and the possibility of developing best practices. As a result of that meeting and with a new grant from the Rose Foundation, CFA created an Identity Theft Service Best Practices Working Group, which included consumer and privacy advocates and members of the identity theft services industry. These best practices, the result of the Working Group's efforts, are intended to provide guidance to the industry and help consumers who are considering identity theft services look for providers that follow good practices.

CFA encourages identity theft service providers to voluntarily follow the best practices and to promote them to others in the industry. CFA recognizes that it may take time to implement the best practices, and that some identity theft service providers may choose to follow some but

¹ *To Catch a Thief: Are Identity Theft Services Worth the Cost?*, March 2009, www.consumerfed.org/elements/www.consumerfed.org/file/To%20Catch%20a%20Thief,%20March%2009.pdf

not all of the recommendations. Some providers may even go beyond the best practices. CFA is not providing a seal of approval or endorsing particular identity theft services, and service providers should not imply that it is. Consumers who are considering identity theft services can use a new checklist² that CFA has developed based on the best practices to help them choose services that follow good practices and meet their needs.

About Consumer Federation of America

The Consumer Federation of America is an association of nearly 300 nonprofit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. For more information, go to www.consumerfed.org.

Identity Theft Service Providers

These best practices are directed at for-profit providers of identity theft services. There are a wide range of identity theft services. Some monitor credit reports and alert consumers to activities such as new accounts opened in their names. Some monitor customers' personal information more broadly, in addition to or instead of monitoring credit reports – for instance, information in commercial and public databases, and in online chat rooms. Some also search “underground” websites that identity thieves use to trade in stolen information. Most services offer some type of assistance for customers who become identity theft victims, from providing advice to taking direct action to resolve their problems. For some identity theft services, fraud resolution is the main benefit they provide. Many services include insurance or guarantees.

Identity theft service providers may offer their services directly to consumers and/or through business partners such as banks, insurance companies or employers. In some cases, identity theft service providers contract with other companies to perform certain aspects of their services, such as providing fraud assistance for identity theft victims. For purposes of these best practices, the identity theft service provider is the company that operates the service in which the consumer enrolls.

Identity theft service providers that follow these best practices should require their business partners and contractors to follow the relevant sections. For instance, if an identity theft service provider contracts with another company to provide fraud assistance to its customers, it should require that the contractor comply with the provisions of the best practices concerning powers of attorney. Similarly, when an identity theft service provider sells its services through business

²*Nine Things to Check When Shopping for Identity Theft Services*, October 2010, <http://www.consumerfed.org/pdfs/9-Things-to-Check-When-Shopping-for-Identity-Services.pdf>

partners such as resellers, agents, affiliates, banks or employers, it should have procedures designed to protect against misleading claims. Such procedures may include published guidelines, periodic audits and/or review of the partners' marketing materials.

Scope of the Best Practices

Some identity theft service providers (as described on page 4) are divisions or affiliates of entities that are engaged in other lines of business. These best practices are directed solely at identity theft service providers, not at the larger entities of which they may be a part. The best practices focus primarily on how identity theft services are promoted. In developing them, the Working Group was mindful of the fact that consumers may have their own expectations about identity theft services and concerns about the use of their personal information. Therefore, it is essential to make available to consumers clear, accurate information about how the services work and the protection and assistance that is provided before they enroll. It is also important to avoid making representations that may, directly or indirectly, mislead consumers. The best practices also seek to encourage other good business practices, including privacy practices. They are organized in three sections: General Guidelines, Information about Programs, and Fraud Assistance.

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.

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.³

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 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;

³ 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.

- 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' websites⁴ and should be provided to new customers in writing or electronically.⁵ Customer service personnel should be trained to answer questions about the privacy policy.

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

⁴ 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.

⁵ 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.

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 policies 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.