Today Consumer Federation of America (CFA) released Best Practices for Identity Theft Services Version 2.0, updating the guidance that it originally issued in 2011 to encourage for-profit identity theft service providers to follow responsible practices. “We revised the best practices to address new trends and issues that have arisen in the identity theft service marketplace and strengthen some of the original provisions,” said Susan Grant, CFA’s Director of Consumer Protection and Privacy. “With security breaches and identity theft cases so much in the news, it’s important for purchasers of these services to understand what they’re getting and for consumers to be treated fairly.”

The revised best practices call for identity theft service providers to:

- Clearly and completely disclose all costs and other material terms before asking consumers to pay and obtain consumers’ affirmative consent to the terms before charging them.

- Clearly disclose the terms of free trial offers, which are frequently used to solicit consumers to try identity theft services for a limited period of time after which they will be charged unless they cancel, and provide simple mechanisms for consumers to cancel.
CFA Revises Best Practices for Identity Theft Services

- Provide clear, easy-to-find, explanations about credit scores when they offer them as part of their programs and not misrepresent the nature of those scores.

- Only share consumers’ financial account and Social Security numbers with third parties to the extent that it is necessary to provide the requested services or as required by law.

- Obtain consumers’ express affirmative consent to provide their personal information to third parties for marketing purposes.

- Refrain from charging consumers for credit reporting and monitoring services if they are unable to deliver those benefits and offer those consumers the option of canceling if the delivery problems cannot be resolved.

There is also a new section in the best practices about data breach services. Businesses, government agencies, and organizations often purchase identity theft services to help individuals whose personal information they hold if that information is breached. Under the best practices, identity theft service providers that seek to sell breach services to such entities should clearly explain the benefits and limitations of their programs and how the features may help breach victims. The data breach provisions also limit the collection, sharing and use of victims’ personal information to that which is necessary to provide the breach services and address how identity theft service providers should approach soliciting those individuals to purchase services after the breach services end.

These revisions were developed in consultation with CFA’s Identity Theft Service Best Practices Working Group, which includes Call for Action; Consumer Action; Mari Frank, Esq.; Privacy Rights Clearinghouse; AllClear ID; Experian; EZShield Fraud Protection; ID Analytics; ID Experts; IDT911; Intersections Inc.; Kroll; Merchants Information Solutions; and Zander Identity Theft Services. Some companies that participated in the revision process are not listed because they are still reviewing the final document and will be added to the list on CFA’s www.IDTheftInfo.org website at a later date. CFA also received informal input from representatives of some government agencies.

“Today’s online consumers unfortunately are exposed to the risk of ID theft and data breaches.
There are many ‘identity theft services’ that market themselves as a response to this uncertainty,” said Linda Sherry, director of national priorities at Consumer Action. “These services offer preventative credit monitoring and/or clean-up assistance for victims of identity theft. CFA’s Best Practices for Identity Theft Services, now featuring a new section about data breach services, and the checklist for consumers, encourage awareness for companies and consumers about what these service can—and can’t—do.”

“We commend the CFA for its unrelenting work in protecting consumers. The implementation of these guidelines will further enhance the image of the identity theft monitoring industry and provide greater customer satisfaction,” said Johan Roets, COO of Intersections Inc. and President of Identity Guard®.

“Identity theft protection is an essential element of consumer protection and remediation following a data breach,” said Michel Bruemmer, Vice President of Consumer Protection for Experian. “That’s why Experian participates in the coalition led by CFA to continually improve best practices for the industry.”

“Unfortunately, the data breach world has gone from lost laptops and misplaced thumb drives to State sponsored hacking and organized crime. It is more important than ever for consumers to be educated and armed with the proper tools to help protect their privacy and identity. We strongly support this effort to identify and communicate the industry’s best practices to help in this effort,” said Bob Gregg, CEO, ID Experts.

“We applaud the CFA working group’s effort to define industry best practices, and in particular, the new guidelines designed to protect the privacy of data breach victims,” said Bo Holland, Founder & CEO, AllClear ID.

“As a major provider of identity and data risk management solutions for insurance, financial institutions and employee benefits organizations, we’re committed to supporting the revised best practices so companies can choose the best identity theft service provider for their customers,” said Matt Cullina, CEO of IDT911. “Adhering to a higher standard service is a core value at IDT911 and part of our mission to help companies strengthen their customer relationships.”
“We are pleased that the companies in the working group support the Best Practices for Identity Theft Services,” said Ms. Grant. “They are leading by example.” Noting that some of the new best practices may take time for companies to implement, Ms. Grant said, “I am encouraged that we’re continuing to move in the right direction.”

The best practices and other resources concerning identity theft, including *Nine Things to Check When Shopping for Identity Theft Services*, are available on CFA’s [www.IDTheftInfo.org](http://www.IDTheftInfo.org) website.