9/7/16

By Susan Grant, Consumer Federation of America Director of Consumer Protection and Privacy

Companies, organizations and agencies that hold and transmit people's personal information should keep it reasonably secure from unauthorized access and use. But what if there is a data breach that exposes the information? How should the breached entity help those affected? Should it offer them identity theft services? If so, how should it choose the provider and what features should it look for to ensure that the services will fit the needs of the victims? To help answer those questions, Consumer Federation of America and its Identity Theft Service Best Practices Working Group , which includes consumer advocates and identity theft service providers, have created a checklist ,
"My company's had a data breach, now what? 7 questions to ask when considering identity theft services."
This isn't intended to be legal advice, however – always consult with an attorney about how to respond to a data breach.

Identity theft services typically include alerting people about possible fraudulent use of their personal information, mitigating the damage, and/or helping them recover from identity theft. In the checklist we explain the different kinds of monitoring and fraud resolution that may be available and that the features of the programs can often be customized to fit particular breach situations. One of the basic questions to ask is whether the service will provide breach victims with information about how to reduce the potential damage – for example, by changing their account numbers and passwords, monitoring their accounts online, and using fraud alerts, security freezes and other tools.

We also suggest asking:

• Are services available 24/7?

• Is there a toll-free number with live operators?

• What response times will the provider commit to?

• Can the service handle multiple languages?

• If monitoring is provided, how quickly are alerts sent?

• Are there specially trained personnel to help victims of fraud resulting from the breach, and will that assistance continue for problems that aren't resolved when the contract ends?

Identity theft service providers may offer other assistance as well, such as helping breached entities to write and/or send notices to the victims and handling other communications. Another thing to consider is whether to have identity theft services lined up in advance in case they're needed. It can be less stressful and save money to pre-negotiate for these services rather than shopping for them in the midst of a breach. The checklist covers how to find reputable identity theft service providers.

Of course, identity theft services aren't necessary in every breach situation. A good rule of thumb is: if the breached entity is required by state or federal law to notify those affected, it should consider offering these services. In interviewing prospective identity theft service providers it's important to describe the types of personal information that have been or could be compromised and ask what features would be most helpful to the victims. We also suggest addressing whether and in what manner the identity theft service provider may solicit the breach victims to buy services during the contract period and/or once it ends. As in any contract, the services and terms should be clearly described and accurately reflect what has been agreed to.

CFA's Best Practices for Identity Theft Services , which was updated last year with input from the working group, and the checklist are intended to encourage good practices in the identity theft service marketplace. There is also a guide for consumers,
Nine Things to Check When Shopping for Identity Theft Services
and much more about identity theft on CFA's
www.IDTheftInfo.org
website.