Protecting Your Customers

Fraud-Fighting Facts

(NAPSA)—Hundreds of data breaches occur every year in the U.S. If your company, organization or agency has a data breach, you need to know what to do to help people whose personal information may have been exposed.

Should you hire an identity theft service provider? If so, how should you choose one? Identity theft services may not be necessary for every breach but if you're going to offer this kind of service, make sure it provides the information and assistance that best fits the needs of those affected.

Consumer Federation of America has created a checklist, *"My company's had a data breach, now what? 7 questions to ask when considering identity theft services,"* to help you make these decisions. This isn't meant to be legal advice, however—always consult with an attorney about how to respond to a breach.

Identity theft services typically alert people about possible fraudulent use of their personal information, mitigate the damage, and/or help victims recover from identity theft. The features of the services vary and can often be customized to fit particular breach situations. One question to ask is whether the service provides information about how to reduce the potential damage that may result from the breach—for example, by changing account numbers and passwords, monitoring one's accounts online, and using fraud alerts, security freezes and other tools.

Other questions to consider include: Are services available 24/7? Is there a toll-free number with live operators? What will the response times be? 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?

Knowing the right questions to ask can help you choose the best services for breach victims.

The checklist explains the different kinds of monitoring and fraud resolution that may be offered. Whether identity theft serices are needed and what features to look for depends on the types of personal information involved and other factors. A good rule of thumb is: if you are legally required to notify the victims of a data breach, consider providing these services. It's wise to retain an identity theft service provider in advance so you won't be scrambling to select one in the midst of a breach situation.

How can you find a reputable identity theft service provider? For the answer to that and other questions about data breach services, go to www.IDTheftInfo.org.