My company's had a data breach, now what?

7 questions to ask when considering identity theft services

When your company, agency or organization holds or transmits personal information, it should keep that data reasonably secure from unauthorized access and use, both internal and external.[1] But if a data breach occurs, what should you do to assist those affected? Do you need an identity theft service provider, and how should you choose one?

This checklist from Consumer Federation of America (CFA) and its Identity Theft Service Best Practices Working Group provides suggestions for questions to ask if you are considering identity theft services to help breach victims. This is not intended as legal advice, however; consult with an attorney before deciding whether to purchase such services, what features are needed, and which provider to select.

The term "data breach" is used here to encompass a broad range of incidents in which personal information may have been compromised, including hacking, accidental disclosure, skimming, insider theft, lost equipment, and careless disposal of documents. Identity theft services may not be necessary in every breach situation, but if you are going to offer them, you'll want to make sure that they provide the breach victims with the information and assistance that best fits their needs.

[1] See information about data security from the Federal Trade Commission at www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security. The nonprofit organization National Cyber Security Alliance also provides information about security at www.staysafeonline.org/business-safe-online/. Another good resource is the Online Trust Alliance Data Protection and Breach Readiness Guide, available at https://otalliance.org/system/files/files/resource/documents/2016-ota-breachguidehr.pdf.

1 What are identity theft service providers?

As described in more detail in this checklist and in CFA's Best Practices for Identity Theft Services,[2] these are companies that provide a range of services which typically include alerting individuals about potentially fraudulent use of their personal information, mitigating the damage, and/or helping victims recover from identity theft. The features of their programs vary widely and can often be customized to fit particular breach situations.

2 Is it a good idea to retain an identity theft service provider *before* a data breach occurs?

Responding to a data breach can be hectic and stressful. Consider having identity theft services lined up in advance in case of a data breach rather than shopping for those services in the midst of one. You may also be able to save money by pre-negotiating for future identity theft services.

3 How do you know whether identity theft services are necessary if a breach occurs?

Whether identity theft services are necessary in the event of a data breach depends in large part on the types of personal information involved and the circumstances in which the breach occurred. Most states have data breach notification laws, some of which require offering identity theft services in certain breaches, and there are also federal laws that may apply.[3] These laws vary in terms of the types of entities that they cover and what triggers a requirement to provide notice, and to whom. Be aware of the data breach laws that apply to you. A good rule of thumb is: if you are legally required to notify the victims of a data breach, you should consider providing them with identity theft services.

---

[2] On page 4 of CFA's Best Practices for Identity Theft Services, identity theft service providers are described as follows: 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" Web sites 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 service providers, fraud resolution is the main benefit they provide. Many services include insurance or guarantees. See www.consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf.

[3] Sources for information about state data breach notification laws include: www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf and www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf. The chart at www.steptoe.com/assets/htmldocuments/SteptoeDataBreachNotificationChart.pdf has state and federal laws.

4 What features of identity theft services should you look for to help breach victims?

The particular features of identity theft services that are most helpful to breach victims will vary according to the types of personal information that were compromised. In interviewing identity theft service providers, describe the types of information that have been or could be compromised and ask them what features would best meet the needs of those affected. They will need to have a thorough understanding of the situation to determine the specific features that you may want to offer.

Information for breach victims

You should always ask whether the identity theft service provides victims with information about how they may be able to reduce the potential damage that may result from the breach. For example, this could include tips about:

- Changing compromised account numbers.
- Re-setting and maintaining strong passwords.
- Monitoring their accounts online and reviewing statements promptly to detect unauthorized charges or debits.
- Accessing and checking their credit reports at www.annualcreditreport.com.
- Recognizing and avoiding "phishing," particularly attempts to exploit the fact of the breach.[4]
- Using fraud alerts, security freezes and other tools that may be appropriate in the situation.

The Federal Trade Commission provides guidance on what to do if one's personal information is lost or stolen.[5] Identity theft victims can use www.identitytheft.gov to report identity theft and get a customized recovery plan.

Other general questions to ask about the service

- ✓ Are the services available to breach victims 24/7?
- ✓ Is there a toll-free number, with live operators to answer frequently asked questions?
- ✓ What response times and other service levels can the service commit to?
- ✓ Can the service handle multiple languages?
- ✓ If monitoring is provided, how quickly are alerts about possible fraud sent, and are there multiple options to receive them?
- ✓ Are there specially trained personnel to assist victims in the event that fraud occurs as a result of the breach?
- ✓ Will the service continue to help victims with fraud that resulted from the breach but has not been resolved by the time your contract ends?

Monitoring

Monitoring, a common feature in many identity theft services, can help detect if someone's personal information is being used or at risk of being used for fraudulent purposes. There are many different types of monitoring. It is important to note that there is no guarantee that monitoring can catch every instance of fraud that it is designed to try to detect.

[4] See information from the Federal Trade Commission about phishing at www.consumer.ftc.gov/articles/0003-phishing.
[5] See https://identitytheft.gov/Info-Lost-or-Stolen.

- Credit monitoring is useful to detect certain kinds of new accounts that are opened using the breach victims' personal information, such as new credit cards, charge cards, auto loans and mortgages. If Social Security numbers have been compromised, credit monitoring is one of the features that you should consider because they are often used to open new credit accounts.
- Credit monitoring may also alert victims to possible fraud when accounts that have been sent to collection are reported, including accounts that don't typically appear in credit reports, such as utilities, telecommunications or health care services. In addition, there may be options for breach victims to be notified when there are anomalies in their account balances, credit limits or credit use. Ask what the credit monitoring will cover.
- To improve detection of existing account takeovers, fraudulent applications for government benefits, impersonating breach victims in legal proceedings and other possible uses of compromised data, you may also want to look for services that monitor public records, proprietary commercial databases, change of address records and other databases. You may want to consider this type of monitoring when Social Security numbers have been exposed in a breach since they can be used for many different fraudulent purposes.
- If only credit card or debit card numbers were compromised, the breach victims should be advised to set up alerts on those accounts. Most card issuers will provide these alerts to customers at no charge. In addition, services that monitor "the dark web" to detect if that information is being offered for sale and alert the accountholders can be helpful.
- This type of monitoring can also be useful to detect if Social Security numbers, passwords and other credentials are being traded on the Internet. Breach victims should always be advised to re-set passwords if they have been compromised, however, and to consult with their financial institutions or other companies with whom they have accounts to determine the best course of action if it appears that the account numbers may have been exposed.

Fraud resolution

Fraud resolution is another feature to consider offering. Before you contract with an identity theft service provider, you'll want to be certain that victims will be able to access resolution services promptly and easily. It's also important to know what types of assistance will be provided to ensure that the victims can get the help they need.

Ask the service provider exactly what the assistance that it can offer to the breach victims would entail. Advice for victims from trained personnel is an important feature of any good identity theft service. For example, with the correct advice about the steps to take, victims can usually resolve problems with fraudulent charges to their credit cards themselves relatively easily.

In some cases, more hands-on assistance may needed, such as contacting creditors, law enforcement authorities, or others on behalf of victims. If the compromised data could lead to problems that are complex and difficult to remedy, such as debit card or other types of bank account fraud, stolen tax refunds, medical identity theft, or employment fraud, seek assurances that the identity theft service provider has expertise in the relevant areas and can provide the help that the victims will need.

5 What other kinds of assistance might identity theft services provide in breach situations?

Some identity theft service providers will help you respond to a breach, including writing and/or sending the notifications to those affected by the breach. If you are interested in this kind of assistance, ask what kind of experience they have in this regard. A well-written notice can reduce call volume and the potential for negative reactions, and encourage victims to take advantage of the services that will be provided. The breach notice should be in plain language, clearly describe the services that are being offered, and explain how victims can access the services. Details of the services and how they can help the victims should be made easily available.

Identity theft service providers may also be able to help you handle calls and emails asking for general information about the breach. If desired, you can work with them on scripts to use. In addition, they may provide you with advice about FAQs and other helpful information for your website. Keep in mind that you should never rely solely on advice from an identity theft service provider; always consult with legal counsel on the wording of breach notifications and other steps that you should take in response to the breach. Consider retaining an attorney that specializes in helping organizations respond to breaches.

6 How can you find reputable identity theft service providers?

An insurer, lawyer or consultant that works with your enterprise to deal with breach situations may have suggestions for identity theft service providers to use. You can also do research online. Be aware that there are many organizations that offer "ratings" for identity theft services. Some of them are independent and impartial, others are "pay-to-play." Ask the identity theft service providers that you are considering for references from clients they have served in similar breach situations. Checking their complaint records and ratings with the Better Business Bureau is another good idea. If service providers have customer satisfaction ratings based on independent assessments of their services, that information can also be helpful. Keep in mind that if you have insurance for cybersecurity risks or other liabilities, it might cover identity theft services in the event of a breach, and the policy may name a specific identity theft service provider or offer a list of providers from which to choose.

CFA's Best Practices for Identity Theft Services encourage identity theft service providers that are seeking to sell breach services to clearly explain the benefits and limitations of their programs and how the features may help the breach victims. The best practices also caution them against overstating or misrepresenting, directly or by implication, how the features of their programs may help the victims.

If the claims being made seem exaggerated or it is unclear whether the features of the service will adequately meet the needs of the breach victims, look for another identity theft service provider.

7 What else should you think about when considering contracting for identity theft services?

As with any business contracts, you'll want to make sure that the services are clearly described in your provider agreement and the terms accurately reflect your expectations. You may also want to

consider including provisions that address whether and in what manner the identity theft service provider may solicit the breach victims to buy services during the contract period and/or purchase services once it ends.

The Data Breach Services section of CFA's Best Practices for Identity Theft Services provides guidance for identity theft service providers in this regard. Furthermore, under that section, identity theft service providers should only ask the breach victims for the personal information that is needed to provide the services and only use the information for that purpose. While it may be necessary to share breach victims' personal information with affiliates or third parties in order to provide the services, the identity theft service providers should share the information only for that purpose and never sell it to others.

Whether you are contracting for identity theft services in the event of a breach or to give your customers or employees as a benefit, CFA encourages you to look for identity theft service providers whose practices are aligned with its Best Practices for Identity Theft Services. Ultimately, the quality of the identity theft services you offer and the behavior of the service provider will reflect on you. Choose the service, and the features of the service, that will best fit the needs of those who may use it.

The Consumer Federation of America (CFA) is an association of non-profit consumer organizations that was established in 1968 to advance the consumer interest through research, advocacy, and education. Today, nearly 300 of these groups participate in the federation and govern it through their representatives on the organization's Board of Directors.