

Credit protection options in the United States

White paper

Consumers who wish to help protect themselves from being victims of financial identity theft have various options available to them to do so. This white paper summarizes those options, and provides factors to consider when choosing among them. It is particularly advisable for a consumer to take action to protect himself from financial identity theft if his social security number has been subjected to unauthorized access by someone who may use it for unauthorized purposes.

Consumer information that is shared with third parties such as retailers and healthcare institutions is also at risk of breach or theft. These third parties may have responsibilities under statute to respond in situations where such data is compromised. This white paper summarizes those situations and looks at the response required as well as detailing some of the options that may be available to a company looking to 'make good' on a data breach or identity theft.

What is a credit report and what does it contain?

A credit report is a report that can be obtained, for a fee, by a company from a credit reporting agency about a consumer's credit accounts and history. For example, before lending money to a consumer, a financial institution usually obtains a credit report on the consumer to determine the consumer's credit-worthiness. A credit report may contain:

- the consumer's name, current and previous addresses, telephone number, reported variations of the consumer's social security number, date of birth, and current and previous employers
- information about the consumer's credit history (including each line of credit that is open at the time of the report, as well as credit lines that are closed); this information includes, for example, the date the credit account was opened, the credit limit or loan amount, the balance, and the monthly payments and payment pattern under the account
- requests for credit reports made by third parties (such as creditors, prospective employers, prospective landlords, etc.)
- public information such as overdue child support, bankruptcy and lien records
- collection agency accounts

Since credit reports contain a list of the credit accounts that are open under a consumer's social security number, they can be used by a consumer to detect whether unauthorized credit accounts have been opened under his name. Additionally, since credit reports contain a list of the consumer's addresses as reported by creditors, reports can also be used to detect whether there has been an unauthorized change of address made on one of the consumer's accounts.

Each consumer has the right to receive one free credit report per year from each of the three national credit reporting agencies (Experian, Equifax and TransUnion). A consumer can request a report from each of the credit bureaus at the same time, or he may stagger his requests throughout the year.

For instructions on how a consumer can request a free credit report from Experian, Equifax or TransUnion, see www.annualcreditreport.com.

What is the purpose of a fraud alert and how do they operate?

A consumer who is concerned about an unauthorized individual opening up a line of credit under his social security number may elect to place a "fraud alert" in his credit file. A fraud alert is a message that credit issuers receive when they request a consumer's credit report, which warns them that there is a possible fraud associated with the account and gives the creditor the consumer's phone number to call the before issuing new credit.

A consumer does not have to call all three credit reporting agencies in order to place a fraud alert with all three of them. Instead, a consumer can contact one of the agencies to place the fraud alert, and the fraud alert will then automatically be placed with the other two agencies as well.

An initial fraud alert lasts 90 days, unless removed earlier by the consumer. At the end of the 90 days, the consumer can renew the fraud alert for an additional 90 days (and can continue to renew every 90 days thereafter), but the consumer is required to proactively renew the fraud alert every 90 days by contacting one of the three credit reporting agencies. If the consumer does not renew the fraud alert, it will automatically expire.

A consumer who has actually been a victim of identity theft (i.e., unauthorized financial accounts have been opened in her name) has the right to place an extended fraud alert on her credit file, which will automatically remain on her credit file for seven years. To place an extended fraud alert, a police report or similar law enforcement report is required.

While having a fraud alert does not prevent or hinder a consumer's activity under his existing credit accounts, it can slow down the process of increasing a line of credit, or opening up a new credit account. The delay is caused by the creditor's actions to verify that the individual who is attempting to increase or open the line of credit is, in fact, authorized to do so. This involves calling the phone number that was given by the consumer to the credit reporting agency when placing the fraud alert.

Why might a consumer elect to place a credit freeze on their credit file?

In a large majority of states, consumers have a statutory right to place a credit freeze on their credit file. In addition, all three of the national credit reporting agencies (Experian, Equifax and TransUnion) allow consumers to place a credit freeze on their credit files regardless of whether they live in a state that has enacted a credit freeze statute. In most cases, the consumer is required to pay a fee to each of the credit reporting agencies in order to place a security freeze. The fee per reporting agency varies by state, but is typically between \$5-\$15.

A credit freeze prohibits a credit bureau from releasing a credit report to a creditor unless the consumer approves of the release through the use of a pin number that is issued to the consumer upon the initiation of the credit freeze. This helps to prevent unauthorized individuals from opening up credit accounts under the consumer's social security number, since most creditors would not be willing to issue credit to an individual without first checking the individual's credit report.

Once a credit freeze is in place, it must be lifted in the event that a consumer desires to open up a new line of credit or, in some cases, increase an existing line of credit. There may be other types of account changes that would also require the freeze to be lifted. A consumer can lift the freeze using the pin number that was issued to him by the credit reporting agency when he placed the security freeze on his account. A freeze can be lifted for a particular period of time or, in some cases, for a particular creditor. It may take up to three days to lift a credit freeze. Therefore, obtaining instant credit is not possible when a consumer has a credit freeze.

Since the instructions for how to establish a credit freeze differ from state to state, and also between the three credit reporting agencies, consumers must contact each of the three national credit reporting agencies individually for instructions.

Why should US citizens check their social security insurance statements?

Each U.S. citizen who has a social security number receives a written statement from the Social Security Administration once per year. The Social Security Statement sets forth how much reported income was earned by the consumer each year since the first year that the consumer earned reported income. In addition to the annual statement which is automatically sent to each social security account holder each year, a consumer can also request a Social Security Statement any time by completing an application and submitting it to the Social Security Administration.

A consumer who is concerned that his social security number may have been used by an unauthorized individual to obtain employment may check his most recent social security statement (or request a new one) to confirm that the amount of money that is reported on the statement as having been earned during a specific year is accurate. If the number reported is too high, it may mean that an unauthorized individual used the consumer's social security number to obtain employment.

What does credit monitoring entail? Why might an insured elect to provide credit monitoring services to their customers? What options are available to them?

A consumer who is concerned about being a victim of financial identity theft may wish to pay a company, such as one of the three national credit reporting agencies, to monitor his credit reports and credit activity, and notify him if anything out of the ordinary occurs. This service is known as credit monitoring service.

Companies that offer credit monitoring services often offer several different levels of service, with the most comprehensive service being the most expensive. The differences between the various levels of service include, for example, whether correspondences are made via postal mail or email, and whether all three of the credit reporting services are monitored, or just one of them. Also, the amount of customer service that is afforded to the consumer differs depending on what level of service the consumer is subscribed to, and the more expensive levels sometimes include identity theft insurance.

When a company experiences an information security breach in which individuals' social security numbers were compromised, the company may elect to pay for credit monitoring services for such individuals. To do this, the company would negotiate a master credit monitoring agreement with a company that provides credit monitoring services. The types of terms that the company might negotiate include, for example: (i) what level of credit monitoring services will be offered to the individuals, (ii) the price the company will pay for the credit monitoring services on behalf of the individuals, (iii) whether the company will pay for each credit monitoring offer that is extended to an individual or only for the individuals who actually accept the offer by subscribing to the service (the unit price will be higher in the later pay structure).

Contact information for three national credit reporting agencies

Trans Union: 1-800-680-7289 (<http://www.transunion.com>)

Experian: 1-888-397-3742 (<http://www.experian.com>)

Equifax: 1-800-525-6285 (<http://www.Equifax.com>)

In what circumstances are companies required to notify individuals that their data has been the subject of a breach?

In the United States, a large majority of states have enacted laws that require companies that have suffered a data security breach to notify the individuals whose sensitive personal information has been compromised. There are also some industry-specific federal laws that impose similar requirements. Although each of the laws are different, and contain their own anomalies, in general, notification obligations are triggered when certain types of sensitive personal information have been compromised. Such information includes, for example, an individual's name along with his or her social security number, driver's license number or financial account number. Some laws also require notification when additional types of information is compromised, such as medical information, date of birth, and mother's maiden name.

How does the breach notification process work? What are the typical costs involved?

When a company has suffered a breach of security of sensitive personal information belonging to its individual customers or employees, it is often required to notify those individuals of the incident so that they can be "on guard" for identity theft. Companies must notify individuals using any of several possible methods, depending on the circumstances, for example, by postal mail, telephone, email, state-wide media and/or web site notice. The means by which a company is required to notify individuals of a breach depends on the jurisdiction, the number of individuals to be notified, the cost of notification, and other factors that differ from state-to-state.

The costs of notification depend on the means of notification. For example, the costs involved in notification by postal mail include the costs of printing the notifications, envelopes, and postage. A mail house is often retained for this purpose. The cost of printing depends on whether the notice letters will be personalized or not. (The industry "best practice" is to personalize notification letters.) Often, when a company does not have current contact information for the individuals, there is a cost involved in obtaining the contact information from a data aggregator. Finally, in almost all cases, a toll-free number is provided in the notification letter for individuals to call with any questions they may have about the incident. Companies usually retain an outside call center to handle the incoming calls.

What does identity theft mean? What are the different types of identity theft?

There are several different types of identity theft, each of which can be achieved using different types of information.

In a sense, when a thief makes unauthorized use of a person's credit card, the thief is essentially assuming the identity of the victim, which can be seen as a form of identity theft. In some cases, a thief can make a purchase using a victim's credit card using only the victim's credit card number. In other cases, the thief may also need the victim's name and, sometimes, card security code number.

Another form of identity theft is referred to as "new account" identity theft. This is when a thief opens up a new credit account under a person's identity. In this case, since the thief uses the victim's social security number to open the account, the account will appear on the victim's credit report. Also, if the thief ultimately does not pay the amount he owes on the account, the victim may receive demands from collections agencies, and his credit report will reflect negative activity which may hinder the victim's ability to obtain new credit accounts. A thief can open up a new credit account under a person's identity using the person's name, address, social security number and other authentication information. Usually, a thief starts with a limited amount of information about an individual obtained from one source (perhaps a theft), and then builds on that information using additional sources, social engineering techniques and pretexting, until the thief has obtained enough information about the person to open up a new credit account under the person's identity.

A third form of identity theft is referred to as "medical identity theft." This is when a fraudster obtains medical services at a hospital, health care clinic, or other health care provider, using another person's medical insurance. Depending on how careful a health care provider is to verify a patient's identity during the intake process, a fraudster may be able to use a victim's medical insurance to obtain medical services using as little as the victim's medical insurance ID number. In some cases, a fraudster may manufacture a counterfeit medical insurance card using stolen information, and then use that card to obtain medical services.