Published on *Privacy Rights Clearinghouse* (https://www.privacyrights.org)

Identity Theft Monitoring Services [1]

Posted Jul 01 2008
Revised Sep 21 2018

1. Introduction

Hardly a day goes by without hearing about someone becoming a victim of identity theft or learning about another data breach. According to Javelin Strategy & Research's February 2018 Identity Fraud Study [2], fraudsters stole $16.8 billion from U.S. consumers in 2017. PRC's Chronology of Data Breaches [3] documents over 8000 data breaches affecting U.S. consumers since 2005.

Faced with these alarming statistics, many consumers have turned to identity theft monitoring services for protection. We use the term "identity theft monitoring services" in its broadest sense. Many of these services only provide credit report monitoring. Some provide other monitoring services in addition to checking your credit report. For example, they may monitor information in commercial and public databases, and in online chat rooms. Some may also monitor underground websites (the so-called "dark web") that identity thieves use to trade in stolen information. Some identity theft monitoring services do not include credit monitoring at all.

Most identity theft monitoring services include a menu of additional services ranging from credit scores, insurance, identity theft resolution services, and access to your credit report. There may be an additional charge for these services.

Identity theft monitoring services may sound like a good way to protect your good credit and your good name. However, it is important to note that these services vary tremendously. Some of these services are overpriced and are not worth the money that they cost.

2. What types of identity theft can credit monitoring services protect against?

Credit monitoring services protect primarily against new account fraud. This form of fraud occurs when a criminal uses your personal information to open credit card, mobile phone, or other financial accounts using your name, Social Security number, and other personal information. New account fraud can be difficult to detect because the criminal generally has billing statements sent to an address other than your real address.

It may take some time before you become aware of new account fraud. You might learn that you are a victim when you apply for a new credit account and are rejected because an imposter has opened accounts in your name, giving you a low credit score. Or you might be tipped off when you are contacted by a debt collector for a past-due account that is not yours.

Credit monitoring does not actually stop the opening of new accounts. But it usually enables you to learn about the fraudulent accounts sooner than it takes for debt collection companies to track you down.

Some monitoring services may provide you with a false sense of security because of holes in coverage. For example, a service may only check with one credit bureau rather than all three, or may fail to report activity in inactive accounts. Unless the service specifically states that it will be monitoring all three credit bureaus (Equifax, Experian, and TransUnion), you should assume that

only one bureau is being monitored.

3. What types of identity theft are *not* covered by monitoring services?

Most monitoring services *cannot* effectively protect against the five types of fraud described below. Some of the more comprehensive services may be able to provide *limited* protection against these other types of fraud. Generally, services that claim to provide more comprehensive protection monitor online chat rooms, blogs, and news sources to look for evidence of criminal activity. However, there is no assurance that a particular fraudulent activity will become the subject of an online discussion. The ability of such enhanced services to protect you from fraud is as yet unproven.

In our opinion, most identity theft monitoring services are unable to provide anything close to complete protection for the following kinds of unlawful activity:

- **Existing account fraud.** Existing account fraud occurs when an imposter uses your current accounts (ones that you already know about) to commit fraud. For example, an imposter could use your credit card account number to make a purchase from an online vendor, or your bank account number to make a withdrawal. This is also referred to as "account takeover" fraud. You generally learn of such fraud by carefully reviewing your monthly account statements. Some financial institutions offer services that can send you an email or text message if a transaction posts to your account.

- **Debit or check card fraud.** Debit or check card fraud occurs when an imposter uses your debit card or check card (or a "cloned" card or the information from your card) to remove money from your bank account. The imposter does not need to know your PIN because he or she will be able to use the card for an "off-line transaction." For more information, see PRC's guide [4] on debit cards.

- **Social Security number and tax refund fraud.** This form of fraud occurs when an imposter uses your SSN to obtain employment, for tax reporting purposes, or for other illegal transactions. For example, an undocumented worker might use your Social Security number to obtain employment. Or an imposter might use your SSN to avoid paying taxes on their income. A rapidly growing problem is identity theft-related tax refund fraud [5] using stolen SSNs. For more information, see PRC's guide My Social Security Number - How Secure Is It? [6]

- **Criminal identity theft.** Criminal identity theft occurs when an imposter gives another person's name and personal information (or counterfeit documents) to a law enforcement officer during an arrest. Frequently, the imposter fraudulently obtained a driver's license in the victim's name and provides that identification document to law enforcement. Or the imposter, without showing any photo identification, uses the name of a friend or relative.

  In many cases, the imposter is cited for a traffic violation or for a misdemeanor violation and is immediately released from the arrest. If the imposter then does not appear in court at the appointed date, a warrant of arrest will be issued under the victim's name. If at a later date the victim is stopped for, say, a traffic violation, he or she may be arrested because of the outstanding bench warrant. In other cases the imposter is arrested, booked, and convicted of a felony. The victim's information is then recorded in criminal records files compiled by local law enforcement, the state Department of Justice, and/or the FBI.

- **Medical identity theft.** Medical identity theft occurs when an imposter uses an individual's name and/or other information (often insurance information) to obtain or make false claims for medical goods or services. Medical identity theft may result in erroneous entries being entered into an existing medical record, or the creation of fictitious medical records in the victim's name.

  This potentially can have fatal consequences for the victim. For example, in an emergency room setting, the victim may be unconscious at the time of treatment. If the victim's medical record reflects the imposter's blood type, allergies, medications, or other medical conditions, health care providers may make dangerous errors. Read more about medical identity theft at the World Privacy Forum's Medical Identity Theft Page [7].

4. What is the best free alternative to monitoring services?

Consumers can place a security freeze on their credit files at the credit reporting agencies (Equifax, Experian, and TransUnion) at no cost. This is a great alternative to credit monitoring and best of all it's free! With a freeze in place, you can prevent *new creditors* (such as a credit card company or lender) from seeing your credit reports. The freeze prevents fraudulent new accounts because new creditors are not able to check your credit report. Requests for access to your credit file will be denied. Most creditors will not issue new credit if they cannot see the consumer's credit report.

You must separately request a freeze from *each* of the three major credit reporting agencies in order to be fully effective. The websites of each of the credit reporting agencies provide instructions for placing a security freeze:

- Equifax [8]
- Experian [9]
- TransUnion [10]

If you want to apply for new credit, you can remove a security freeze temporarily. You can also permanently remove a freeze.

A security freeze does not apply to credit checks for:

- Employment or background screening purposes
- Tenant screening
- Insurance underwriting
- Identity verification purposes

Security freezes will not impact your credit score or your relationship with your *existing creditors*. Any existing creditor can continue to see your credit reports in order to periodically review your account.

A security freeze cannot stop misuse of your existing bank or credit accounts. You still must check your accounts for any errors or fraudulent activity.

Security freezes should not be confused with credit locks. Credit bureaus often encourage consumers to use a credit lock rather than a security freeze. While a security freeze provides protection that is governed by law, locks are governed by your contractual agreement [11] for each credit bureau. Having a contractual agreement is not as good as having protections under law. For example, the contract may include provisions that you may be better off not agreeing to, such as an arbitration agreement.

5. What are the other free alternatives to paying for monitoring services?

There may be several, depending on your situation:

- **Fraud alerts.** You are entitled to place a free fraud alert on your credit reports even if you have not yet become a victim of identity theft. You can do this by phone, online, or in writing. A fraud alert places a “red flag” on your credit reports, alerting potential creditors to take extra precautions before extending credit. Typically, creditors will call you to verify your identity before issuing any credit.

  When you request a fraud alert from one bureau, it will notify the other two for you. Your credit file will be flagged with a statement that says you may be a victim of fraud and that creditors should take additional steps to verify your identity before extending credit. The federal Fair Credit Reporting Act (FCRA) enables you to place an initial fraud alert for one year. You can continue to renew a fraud alert indefinitely. You may cancel the fraud alerts at any time.

  - Equifax fraud alert [12] and fraud department (888) 766-0008
  - Experian fraud alert [13] and fraud department (888) EXPERIAN (888-397-3742)
  - TransUnion fraud alert [14] and fraud department (800) 680-7289

  An *added benefit* of a fraud alert is that it entitles you to free copies of your three credit reports each time the fraud alert is established. This is *in addition* to your right to your free annual credit reports. For more information, visit the official annual credit report website [15] and read the Federal Trade Commission’s guide [16].

- **Extended fraud alerts.** Victims of identity theft [17] and military personnel [18] away from their duty station may be eligible for longer fraud alerts.

- **Free credit monitoring from financial institutions and other organizations.** Some banks, credit unions, auto clubs, and other organizations offer free monitoring services with their credit cards or other services. Sometimes, they will use a free basic service as a marketing tool to "upsell" you to a fee-based premium service.

  Credit Karma [19] offers free credit monitoring. Their service utilizes *TransUnion and Equifax*, two of the three major credit reporting agencies. Credit Karma's advertisers pay for the credit monitoring service. Consumers are not charged for the service and no credit card is required. You should be aware that the other major credit bureau, Experian, is *not* included in this service. (No endorsement implied.) You can also see your *TransUnion* and *Equifax* credit reports and credit scores on this site at no charge.

Credit Sesame [20] also offers free credit monitoring. Their service utilizes *Experian*, one of the three major credit reporting agencies. Credit Sesame's advertisers pay for the credit monitoring service. Consumers are not charged for the service and no credit card is required. You should be aware that the other two credit bureaus, TransUnion and Equifax, are *not* included in this service. (No endorsement implied.)

- **Data breaches.** Victims of data and security breaches are often offered a year or more of of free credit monitoring as "compensation" for the breach. It's important to understand the limitations of such free offers. Make sure that all three credit bureaus are included in the monitoring and that you automatically receive alerts when there is any activity in your credit report.

6. What features should you look for when purchasing a monitoring service?

The PRC believes that identity theft monitoring services are not necessary for many consumers. The free alternatives suggested above often provide adequate protection for the typical consumer. However, there may be circumstances where a consumer desires the psychological security of a monitoring service or when particular circumstances might make monitoring desirable.

- **Tip:** Before considering paying for a monitoring service, think about whether a free security freeze (described above) might provide better protection.

Remember that most monitoring services only have the capability to inform you of an identity theft *after* it occurs. A security freeze can *prevent* new account fraud *before* it happens. Monitoring does not actually stop the opening of new accounts. You will just find out about the fraudulent accounts sooner. Monitoring services may provide a false sense of security because there may be holes in coverage. For example, a service may only check with one credit bureau.

If you decide to subscribe to an identity theft monitoring service, be sure to read and understand the product offering carefully. Consider whether the service follows Consumer Federation of America's [21]Best Practices for Identity Theft Services [22]. [22]

Ask these questions when you consider an identity theft monitoring service:

- Does the service provide daily, weekly, or monthly credit monitoring? The better services offer daily or even real-time monitoring.
- Does the service provide credit monitoring at all three credit reporting agencies? Monitoring at only one credit bureau provides insufficient protection because typically a potential creditor will only check with one of the three credit reporting agencies before opening a new account. There is no guarantee that the credit issuer will check the one credit bureau that your particular service monitors.
- Does the service provide you with unlimited access to your credit reports?
- Does the service give you unlimited access to your credit scores? Be aware that monitoring services typically do not provide access to your FICO score, which is the industry leader in credit scores. For additional information on credit scores, read PRC's guide to credit scores [23].
- Does the service consist primarily of services that you could perform yourself at no cost (for example, fraud alerts, credit card pre-screen opt out, the telemarketing do-not-call list)?
- How does the cost of the service compare with other services? Prices vary tremendously and may or may not be indicative of effectiveness of the service that you will receive or the level of services provided.
- Does the service offer additional monitoring services? Some services include Internet newsgroups, search engines, blogs, chat rooms, public records, and online directories that list consumers' information.
- Does the service provide any incidental products such as free computer security software?
- What type of assistance, if any, will you receive to recover from identity theft? The nature of this assistance may vary tremendously from one service to another. Some services may only offer you forms (fraud affidavits) to complete. Others may provide you with individualized counseling services. The best services will actually contact creditors, employers, law enforcement agencies, and others as needed to help your identity theft. A few services may also provide legal services for the most complex identity theft problems.

- Is identity theft insurance included and what does it cover (see below)?

7. Is it necessary to purchase identity theft insurance?

The risk of financial loss from identity theft is generally very low. If you report a loss promptly after discovery and you have not done anything to contribute to the loss, it is unlikely that you will have financial responsibility. You may encounter a few costs in documenting your loss, such as postage, notary, and copying costs, but these are likely to be minimal.

The biggest cost will be your time. Most policies will not compensate you for your loss of time. For this reason, it's unlikely that you need to purchase identity theft insurance.

Some identity theft services include insurance as part of the package. Insurance is a highly regulated product that must be issued by a licensed insurer. If you are obtaining insurance, here are some questions to ask:

- Does the coverage include actual financial losses from the identity theft, the costs of documenting your loss, or both?
- Does the coverage pay you for lost wages?
- Does the coverage include attorney's fees for legal defense when necessary?
- Does the coverage include thefts committed before the policy's effective date, but not discovered until afterwards?
- What is the deductible that you must pay before obtaining benefits and services from the insurance policy?

You might also want to check to see if you are already covered by your homeowner's or renter's insurance. Or check if your insurer may be able to add coverage for a small annual fee.

Note: The Privacy Rights Clearinghouse does not endorse, recommend, or link to any identity theft monitoring services.

Source URL (modified on September 21, 2018): https://www.privacyrights.org/consumer-guides/identity-theft-monitoring-services

Links
[1] https://www.privacyrights.org/consumer-guides/identity-theft-monitoring-services
[2] https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
[3] https://www.privacyrights.org/data-breaches
[4] https://www.privacyrights.org/consumer-guides/paper-or-plastic-what-have-you-got-lose#4
[5] http://www.gao.gov/products/GAO-13-132T
[6] https://www.privacyrights.org/consumer-guides/my-social-security-number-how-secure-it
[7] http://www.worldprivacyforum.org/category/med-id-theft/
[8] https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
[9] https://www.experian.com/freeze/center.html
[10] https://www.transunion.com/credit-freeze/place-credit-freeze
[11] https://www.consumerreports.org/credit-bureaus/why-credit-freeze-is-better-than-credit-lock/
[12] https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
[13] https://www.experian.com/fraud/center.html
[14] https://www.transunion.com/fraud-victim-resource/place-fraud-alert
[15] http://www.annualcreditreport.com
[16] http://www.ftc.gov/bcp/edu/microsites/freereports/index.shtml
[17] https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes
[18] https://www.consumer.ftc.gov/articles/0273-active-duty-alerts
[19] https://www.creditkarma.com/credit-monitoring
[20] https://www.creditsesame.com/
[21] http://www.consumerfed.org/idtheft/CFA-Best-Practices-Id-Theft-Services.pdf
[22] http://consumerfed.org/pdfs/CFA-Best-Practices-Id-Theft-Services.pdf
[23] https://www.privacyrights.org/your-credit-score-how-it-all-adds