

Costly credit-monitoring services offer limited fraud protection

You can guard against identity theft better by taking other steps

An excerpt from **ConsumerReports**
MoneyAdviser

Over the last three years, some 49 million Americans were told that their personal information was lost, stolen, or improperly disclosed by government agencies, banks, or various other companies, according to a recent survey by Harris Interactive. Although most respondents said that nothing happened as a consequence, 19 percent reported that the breaches led to unauthorized credit-card charges, bank-account losses, or other forms of identity fraud.

The solution, say the nation's three major credit bureaus, is credit monitoring. For \$60 to \$180 a year, Equifax, Experian, and TransUnion claim they'll protect you from identity theft by regularly watching for changes in your credit report. About 24 million customers have signed up, according to Javelin Strategy and Research, a California-based company. Unfortunately, our analysis shows that as currently designed, such services are often overrated, oversold, and overpriced.

Credit monitoring is sold by stoking consumers' fear of fraud. The hardest push is reserved for those who have already been victims of data-security breaches. Prior victims are more likely to buy monitoring services than nonvictims, making them prime marketing targets, says Mary Monahan, a partner at Javelin.

Equifax says that "monitoring your credit reports for changes is one of the best ways to protect yourself from identity theft." But that's not the whole story. Fact is, credit-report monitoring watches only one window through which an ID thief may escape with your good name.

A newer type of service, ID fraud prevention and detection, keeps an eye on other windows by trawling Internet chat rooms and directories and by sifting through online public records for signs of Social Security number fraud, stolen credit-card account trafficking, and other types of ID theft. Some of these services also come with limited credit-report monitoring. These ID fraud prevention and detection services are too new for us to properly assess now, but a recent report by the Gartner Group, a Connecticut-based consulting firm, predicts that they may "overtake credit-report monitoring as an effective identity-theft tool by year-end 2009." That's further indication of the limited nature of credit monitoring.

Neither the Federal Trade Commission nor consumer groups including Consumers Union, the Identity Theft Resource Center, and the Privacy Rights Clearing House recommend or endorse credit-monitoring services. If you're tempted to sign up, however, you should know that credit-bureau monitoring services have the following limitations.

There's no protection against theft of your Social Security number. You may think that every person's credit information is solidly anchored to a universal identifier--a Social Security number (SSN)--so that credit-file data about the Visa cards of Mary Smith living in Peoria, Ill., won't get mixed up with those of all the other Mary Smiths around the country. You might also assume that Peoria's Smith can keep tabs on who's using her SSN by checking her credit report.

In fact, says Melody Millett, a database analyst in Overland Park, Kan., "I can apply for a credit card tomorrow using my name and your Social Security number, and you won't learn about the new account from your credit report." That's because credit data with your SSN on it may not be automatically routed to your credit-bureau file in a timely way. For that reason, a credit-monitoring service won't pick up on and alert you to a fraudulent account like the one Millett describes.

Millett speaks from painful experience. In 2001 and 2002, an illegal immigrant in California financed two vehicles through Ford Motor Credit using one of his aliases and the SSN of Millett's husband, Steven, according to court filings. The Milletts did not find out about the fraud until 2003, when Ford Motor Credit refused to give Steven an electronic bill-payment identifier for his car loan because someone else was already using his SSN. Further investigation revealed that the ID thief had been using Steven's SSN to obtain credit and employment since at least 1989.

Other people can use your SSN to obtain credit because of a credit-bureau practice of creating "temporary fragmented files" when creditors file account information with your SSN but with a different name, address, and date of birth, according to a 2004 Federal Trade Commission report. Bureaus hope to later link the odd data in the separate file with the correct credit file using "matching algorithms" and other information. For example, a mismatch might occur when a woman changes her name because of marriage, which would become obvious by further name updates.

That doesn't explain why the bureaus didn't flag the fraudulent use of Millett's SSN. As it turns out, if enough new data come in with an SSN that matches the thief's name and address, the credit bureaus effectively give the new identity their blessing and proceed to sell the fraudulent information to prospective creditors.

As long as the credit bureaus keep your credit file separate from that of the ID thief, your credit report and monitoring service will never pick up the new accounts. But credit-bureau computers constantly work to match the two files, and when they do, you get penalized for the thief's history. Files can also become mixed when a collection agency comes after you for the bad guy's bad accounts.

Credit bureaus' monitoring services do not alert consumers to others who may be using their SSNs. "Experian has no way to establish ownership of a Social Security number, as the Social Security Administration will not provide that type of validation," says Donald Gerard, an Experian spokesman. "Therefore, we would be unable to determine fraudulent use of one's Social Security number."

Although they may not know the rightful owner of a particular SSN, Experian and TransUnion do sell lists of names that use the same numbers to collection agencies and other businesses in their "Social Search" and "TRACE" products.

The Milletts, meanwhile, have spent more than \$12,000 in legal fees plus countless hours trying to correct their credit record. They can't get credit, have been shut out of low- and zero-rate financing opportunities, and have been paying \$400 more a year for homeowners insurance because of their damaged credit.

And when creditors began relabeling the ID thief's fraudulent accounts in Steven's name and address, "none of the credit-monitoring products we bought caught it," says Melody. "I've had Credit Manager from Experian, True Credit from TransUnion, and Credit Watch from Equifax." She adds that there was never any notification that Steven might be a victim of identity theft. All three credit bureaus declined to comment on the case.

A spokesman for PrivacyGuard, a credit-monitoring service offered by the Affinion Group, based in Connecticut, told us that the service monitors fragmented files and use of your SSN by others. But we couldn't find any such claim in PrivacyGuard's Web marketing material, press releases, or terms and conditions document. The Affinion Group does, however, claim to provide such tracking with its new fraud prevention and detection service, ID Secure.

Gaps in monitoring and notification leave you exposed. Even if you ignore that first glaring flaw, for a credit-monitoring service to truly protect you, it needs to cover as many information sources as possible. But when we assessed 16 credit-monitoring services, we found 8 that monitor the credit reports at only one of the three major credit bureaus. That is incomplete coverage because creditors do not always report to all three credit bureaus.

Equifax's Credit Watch Silver, Gold, Gold Family, and Score Watch; Experian's Credit Manager and CreditCheck Monitoring (sold through ConsumerInfo.com); TransUnion's Credit Monitoring; and Identity Guard's Credit Protect provide only one-bureau coverage.

Another big hole in the safety net involves the kind of credit-report activity that prompts an alert and how quickly the notice goes out. Some products don't alert you to sudden activity in dormant accounts, unexpected increases in balance levels, changes in existing accounts, or the appearance of a negative public record. And while most do offer alerts about such changes daily or within a day of changes, Equifax's budget Credit Watch Silver takes as long as a week to report a change.

Another serious concern: Built-in delays and deficiencies in how credit information is reported means that it may take a creditor 60 days or more to report a new fraudulent account.

ID theft insurance might prove worthless. Most of the credit-monitoring products that we examined also provide what might seem like a comforting offer: identity-theft insurance that reimburses you for lost wages for time taken off work to deal with fraud; notary and certified-mail costs; long-distance calls to report or deal with a fraud; and even legal fees (with prior approval of the insurer) for defense in collections, removal of erroneous civil judgments, and challenging information on your credit report.

But scrutinize the terms of coverage for loopholes. For example, some insurers exclude coverage for losses that occurred prior to your purchase of the product. It can take months or years for ID theft to be discovered. So if a thief opened a fraudulent account in your name two years ago, you bought monitoring one year ago, and you don't discover the crime until next year when a collection agency hunts you down, your insurance protection and payout might be zero with some policies.