ID THEFT MONITORING SERVICES: WHAT YOU NEED TO KNOW

Fee-based services say they'll protect your identity, privacy, credit, name, and more. Find out what they can and can not do -- and learn what you can do to defend yourself.

What is your identity worth? According to the Global Internet Security Threat Report from Symantec, credit card numbers go for as little as $0.40 on the black market. Complete access to a bank account? Just $10.

Not so long ago, one's identity didn't involve so many dollars and cents. Discussions of privacy seemed better suited to the realm of academic debates or conspiracy theories. Today, unfortunately, the context is too often one of ripped-off consumers, with tales of swiped credit card numbers, false mortgages, and employment fraud leading to many cumulative hours spent, perhaps over years, trying to clean up the mess.

Of course when someone comes gunning for granny's life savings, "good Samaritans" won't be far behind.

Take identity theft monitoring service providers. The pitch? Give us your Social Security number and notification of suspicious identity activity is only an e-mail alert or phone call away. These services, which typically cost $10-$20 per month, offer to guard your identity by monitoring the three credit-reporting agencies (Experian, Equifax, and TransUnion), cell phone applications, government databases, and public information. Some also provide insurance (subject to underwriting, and not valid in every state) to help defray costs associated with recovering from identity theft cases.

Others offer even more. For example, Intersections' Identity Guard ($17 per month for the "Total Protection" plan) says it uses "patented scanning technology" to maintain "daily surveillance of the Internet's 'back alley' chat rooms and news groups" and see if your identity is for sale. Secure Identity Systems ($7 per month) says it "tracks hundreds of databases that use Social Security numbers, including utilities, DMV records, financial institution records, and more."

MyPublicInfo ($80 for a six-month "Public Information Profile") watches criminal records and real estate reports. Debix ($99 per year) automatically calls you at home or on your cell phone the moment someone obtains new credit in your name. LifeLock ($10 per month) requests "that your name be removed from pre-approved credit card and junk mail lists, and we keep making the requests as they expire," so would-be attackers can't swipe credit card offers from your mailbox. According to LifeLock, "we've got your back."

What Monitoring Can -- And Can't Do
More Than 225 Million Records Breached Since 2005

A little identity theft prevention would be nice, especially since over 225 million records containing sensitive, personal information have been compromised since January 2005, according to the Privacy Rights Clearinghouse. Furthermore, the quantity and scale of data breaches appears to be on the rise. For example, a March break-in at an Indiana debt-collection agency led to a missing server containing 700,000 people's personal information, including some Social Security numbers. (The server is still at large.)

More Security Insights

Of course, not every breached record results in a case of identity theft. (Interestingly, an Identity Theft Research Center study found that in almost half of all identity theft cases, the victim believed the perpetrator had been family or a friend.) Yet with breaches on the rise, it may not be a surprise that the incidence of identity theft reportedly increased three-fold in 2007.

Furthermore, identity theft cleanup can be complicated. According to a Federal Trade Commission study of identity theft cases from 2001 to 2006, for the extreme 10% of cases, costs stretched to $1,200 and clean-ups required 44 hours. Thankfully, however, the median time to resolve an identity theft problem was four hours, and "in more than 50% of ID thefts, victims incurred no out-of-pocket expenses," which includes "any lost wages, legal fees, any payment of fraudulent debts, and miscellaneous expenses such as notarization, copying, and postage."

What Identity Theft Monitoring Promises

Monitoring helps with identity theft by actively watching for fraud in your name. "The credit monitoring service notifies you at an earlier stage than you might otherwise know about the fraud, because otherwise it could be months before someone potentially finds out about it," says Paul Stephens, director of policy and advocacy at PRC.

Monitoring, however, won't stop identity theft outright. "With credit monitoring, your report is still potentially seen by people who want to commit fraudulent acts against you," he says. "You'll get an early warning, but you haven't actually prevented them from using the report." At this point, it's also too late to freeze your credit, which prohibits anyone but current creditors from seeing a credit report. This means your personal data is already at large, and may have been used to gain a credit card, cell phone, or even mortgage in your name.

In addition, spotting data breaches may take months, if not (cough, TJX) years. Meaning the proverbial horse left the barn long ago. "The goal in credit monitoring is to monitor new fraud," says Stephens, such as when someone attempts to open new credit in your name. If the credit card account already exists, however, monitoring services won't spot that it's being used inappropriately.

Is Monitoring Worth The Cost?

Caveat Monitor

Not all services or service levels are created equally. Some companies, in fact, only monitor one credit bureau, at least for their basic level of service. So if someone applies for a credit card in your name at Citibank (which uses TransUnion) and your service only monitors Experian, then it won't catch it.

More Security Insights

And some services don't even monitor credit reports. LifeLock, for example, only places a fraud alert on your account, which is "not as strong as a credit freeze," says Stephens. "It merely places a red flag on your credit report that notifies potential creditors that there may be some fraudulent activity here, so take extra steps to verify the identity." Just like verifying the signature on the back of a credit card at a point of sale, however, this verification may not happen.

Under current laws, the LifeLock approach -- acting as a proxy for consumers to place fraud alerts -- may not last long. Experian recently sued LifeLock, saying the company is inappropriately using fraud alerts, which are restricted (per the Fair Credit Reporting Act) for consumers only. According to Experian's complaint, "LifeLock's scheme costs Experian millions of dollars every year in processing large numbers of improper initial fraud alerts, mailing mandatory notices to consumers, and providing free credit reports to consumers who are not eligible for such reports."

Then again, Experian offers its own, competing monitoring service. But it's been under fire from the FTC over its FreeCreditReport.com site, which only provides a free credit report if you sign up for Experian's (not free) service. The FTC says the site is uncomfortably close to AnnualCreditReport.com, which actually does provide free credit reports.

These tangled connections are not unlike the state of the data brokerage market itself. "The idea of monitoring what's on your credit report is a strong idea, however, part of the problem is that sometimes the same people who are selling you this ID theft monitoring are the same credit reporting agencies that ought to be protecting your credit report to begin with," says Guilherme Roschke, a Skadden Fellow for the Electronic Privacy Information Center's Domestic Violence and Privacy Project in Washington. "They shouldn't be selling a service which is to protect you from the chance that they'll be reporting incorrect information in your report, or that they'll be giving out your credit report without [appropriate controls]."

Is Monitoring Worth the Cost?

All of which begs the question: Are these services worth the cost, and more to the point, do they actually protect you from identity theft?

"Our position is that for most consumers -- and by most, we mean well over 99.9% of the people in the country -- they are not," says PRC's Stephens. "If you're talking about spending upwards of $100 per year, we don't think that the typical benefit a consumer is going to derive is worth the cost."

On the other hand, if these services are offered for free, "go ahead and do it," he says. For example, some banks offer free monitoring as a premium account perk. Or, "if you've been notified that you've been the victim of a data breach, the organization will often provide you with a free year of credit breach monitoring."

Free Ways To Monitor Your ID

But monitoring is not necessarily the best way to prevent or even defend against identity theft. "I think a freeze is a much better way to control your credit," says EPIC's Roschke. "It prevents things from happening without your permission. And in many ways, that's better than credit monitoring, because you don't have to keep an eye on it. You've just locked it up."

Five (Mostly) Free Alternatives to ID Theft Monitoring Services

Instead of paying for identity theft monitoring, consumers can roll their own monitoring, prevention, and reaction program, mostly for free. Here's where to start:

1. Watch your credit reports. Everyone is entitled to see a free credit report annually from each of the three credit-reporting agencies (Experian, Equifax, and TransUnion). To obtain yours, see AnnualCreditReport.com.

2. Use credit freezes. A credit freeze (aka "security freeze") locks credit reports so only you or current creditors can see it. It can also be unlocked on a per-creditor basis, for example if you're going to buy a house, car, or get a new credit card.

   The cost is $10 per bureau to place a freeze and $10 to lift a freeze, though this varies by state, and may even be free, especially for senior citizens or victims of identity theft. (For a state-by-state breakdown of costs, see Consumers Union.) This approach is better suited to financially established people, versus younger people who may need fast access to credit.

3. Place fraud alerts. Under the Fair Credit Reporting Act, consumers may place a fraud alert on their credit report for 90 days -- renewable indefinitely -- which warns potential creditors that there's been fraudulent activity. Also available: an extended, 7-year alert, which also excludes you for 5 years from "pre-approved" credit card offers. First, however, you must file an FTC identity theft report.

4. Avoid debit cards. Attacks which steal card numbers via ID-swiping devices -- often installed at gas stations and grocery stores -- are on the

rise. "That information can be sent overseas, and there's a whole industry that makes up fake credit or debit cards," says Stephens. Suddenly, your account may be empty. While credit card losses are typically capped at $50 (if not waived, as long as the financial institution doesn't suspect you of fraud), no such protections exist for debit cards.

5. Look to resolution services. Public agencies and non-profit organizations can help you clean up identity theft for free. Start with the Privacy Rights Clearinghouse, MassPIRG's How to Clean Up Identity Theft, and the FTC's Fighting Back Against ID Theft.

What No Identity Theft Monitoring Can Catch

One word of warning: Credit monitoring, credit freezes, and fraud alerts cannot protect against three kinds of identity theft:

*** Medical ID Theft.** "This is where someone fraudulently uses your insurance information to obtain care in a hospital emergency room," says Stephens. Thanks to the cost of insurance, it's a growing threat, with a grim potential side effect: it creates a fake medical record in your name, perhaps listing a different blood type or incorrect allergies. In a worst-case, emergency room type of scenario, this can be fatal.

*** Social Security Number Fraud.** Undocumented workers may steal your Social Security number for employment purposes. "All of a sudden, you're going to get a W-2 from the IRS that says, why didn't you report this income?" says Stephens.

*** Criminal Identity Theft.** If someone is arrested and has fake credentials in your name, then their fingerprints and resulting criminal record may also end up in your name. "Then they don't show up at the court date, and a warrant goes out on their arrest, and probably what happens is, you get pulled over at a traffic stop, and hey, you have a warrant out against you," says Stephens.

(By Mathew Schwartz, www.InformationWeek.com, May 9, 2008)

http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=207501091&pgno=1&queryText=&isPrev=