

PCWorld

Identity Protectors:

Who Can You Trust?

BY DAN TYNAN

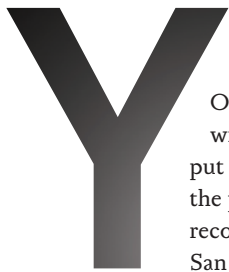
New online services offer to protect you from identity theft, and some claim to help you undo damage after it happens. But when we tested the services, we found that many fall short.

HOW MUCH IDENTITY PROTECTION DO YOU GET FOR YOUR MONEY?

None of the six services we tested qualifies as full-featured. Here's how they ranked, based on offerings and performance.

COMPANY/SERVICE, IN ORDER OF RATING	Rating	Credit alerts and online credit reports	Public record reports	Fraud alert	Online dashboard	Chat room scans	Identity theft insurance	Security software	Comments
Identity Guard "Total Protection" \$17/month or \$170/year www.identityguard.com	Good	Yes	Yes	No	Yes	Yes	Yes	Yes ¹	Full service handles both monitoring and freezes, but interface invites signing up for things you already have.
Debix Identity Protection Network \$99/year ² www.debix.com	Fair	No	No	Yes	Yes	No	Yes	No	Service offers real-time identity verification via phone, though not all creditors take advantage of this.
Suze Orman's Identity Theft Kit \$40 kit www.suzeorman.com	Fair	No	No	Yes ³	Yes	Yes	Yes	Yes ⁴	Software-based kit uses TrustedID for alerts; claims to protect against theft of health insurance records, too.
TrustedID "Identity Freeze" \$13/month or \$110/year www.trustedid.com	Fair	No	No	Yes	Yes	No	Yes	No	This is the only service to manage both credit freezes and fraud alerts. Performed as advertised in our tests.
LifeLock \$10/month or \$110/year www.lifelock.com	Poor	No	No	Yes	No	Yes	Yes	No	The most limited of the services tested lacks online dashboard; fraud alert wasn't set until we followed up.
TrueCredit by TransUnion "3 in 1 Monitoring" \$15/month www.truecredit.com	Poor	Yes	Yes	No	Yes	No	No	No	Service is marred by obnoxious marketing tactics; in our tests it failed to issue alerts in two instances.

¹ Free download of ZoneAlarm Security Suite included. ² Also sold by LoudSiren for \$9 a month. ³ Via partnership with TrustedID. ⁴ Installs antivirus and antispyware software.



YOU CAN'T OPEN a newspaper or a browser without reading about some data spill that has put consumers' personal information at risk. Over the past three years, more than 220 million private records have been lost or stolen, according to the San Diego-based Privacy Rights Clearinghouse. In 2007, 8 million to 15 million Americans had their identities stolen. The odds that it will happen to you are about one in five, according to surveys conducted by the Chubb Group.

Identity theft is a national epidemic, but some firms also see it as a marketing opportunity. In fact, some credit bureaus and banks that facilitated the spread of easy credit—and in the process unwittingly made identity theft a more profitable crime—now sell services to help you avoid having your identity pilfered.

For \$10 to \$20 a month, a company such as LifeLock or TransUnion will monitor your credit reports, alert you if anyone opens an account in your name, and help you recover fraudulent charges. But you can do many of the things these services offer to do, at no cost except for the effort (see “DIY Identity-Theft Protection: A 12-Step Program” on page 3 for details).

To assess the paid services, we signed up with six leading firms. Even services that worked as advertised weren't comprehensive. Only two—Suze Orman's Identity Theft Kit and Identity Guard—offered protection for anything beyond financial fraud. Using any of the services is better than doing nothing, but you may still have to work to safeguard your identity.

Monitoring Your Credit

The keys to your financial identity jangle in the pockets of the Big Three credit bureaus: Equifax, Experian, and TransUnion. When you apply for a credit card, sign up for a wireless plan, or apply for a job, the company you're trying to do business with is likely to request a copy of your credit report. If anyone steals your identity, that person's bad behavior goes on your report, hurting your chances for a loan, a phone, or a job.

Federal law entitles you to a free annual report from each of the Big Three. You also qualify for a free copy if you've recently been denied credit or if you're an identity-theft victim. The bureaus make no money by supplying free credit reports, but they make a lot of money—more than \$1 billion annually, according to Javelin Strategy and Research president James Van Dyke—by selling credit-monitoring services.

For \$5 to \$20 per month, a credit-monitoring service will alert you whenever your report changes. If a thief opens new accounts in your name, you'll usually find out within a few days. Most monitoring services offer online credit reports, online credit scores (showing your chances of obtaining credit), and tools for managing and improving your credit rating.

But a credit-monitoring service won't tell you if someone steals your credit card and runs up huge bills; for that you must check your monthly billing statements. Furthermore, if you receive an alert about a dubious inquiry, you'll have to

identify it as bogus and contact the credit bureaus on your own.

Our real-world tests of two major credit-monitoring services yielded mixed results. First we signed up for TrueCredit's three-in-one monitoring service, which promises to deliver e-mail alerts from all three bureaus for \$15 a month. The first two times our tester tried to open a new credit account, TrueCredit failed to issue an alert. A third test a month later was more successful.

“The likely explanation is that [the bureaus] had not yet completed the processing required on their end by the time the first two inquiries were made,” says Steve Katz, a spokesperson for TrueCredit's parent company, TransUnion.

Using TrueCredit was truly annoying in other ways. Whenever we accessed our account or received an e-mail alert, we had to wade through advertisements for credit scores, low-cost credit cards, and other services.

We had better luck with Identity Guard, whose parent company, Intersections, provides identity-theft protection sold through Citibank, Equifax, GE, and other firms. We signed up for Identity Guard's \$17-per-month Total Protection plan—which provides credit monitoring, credit scores, security software, and public-records searches that identify names, addresses, and property associated with your identity, along with things like licenses, tax liens, and criminal convictions—and it alerted us to every change made in our credit reports.

Unfortunately, we found Identity Guard's interface confusing and its customer service line unhelpful. One particular annoyance: Our account page advertised services already covered under the Total Protection plan, inviting unwary consumers to buy the same services twice under different names. Tim Walston, a senior vice president for Intersections, explains that the ads are provided for people who may want to obtain fresh reports between Identity Guard's quarterly updates.

When Fraudsters Attack

If credit monitoring is a burglar alarm that goes off when someone steals your identity, a fraud alert is a deadbolt that prevents break-ins. At least, that's how it's supposed to work. By law, you can place a temporary fraud alert on your credit report, requiring lenders to verify your identity before issuing credit in your name. And if you tell one credit bureau to set up a fraud flag, it's obliged to notify the other two. But such alerts expire after 90 days. To address the lapses in coverage, companies such as Debix, LifeLock, LoudSiren, and TrustedID will renew alerts every three months for \$9 to \$13 a month.

These services set their alerts in different ways. LifeLock and TrustedID contact the bureaus and set the alert. Debix (which powers LoudSiren) provides its own contact number for lenders. When a creditor calls the number, Debix's automated voice network calls your phone and lets you approve or deny the transaction by entering a PIN. Debix can call up to three numbers until it finds you.

But in real-world tests, our results varied widely. After sign-

ing up for TrustedID, one of our testers applied for instant credit at The Gap. Store employees saw the fraud flag, called the Gap's internal credit division (operated by GE Money Bank), and put our tester on the phone to answer multiple-choice questions about his finances.

Another tester signed up for LifeLock and applied for a card at a different Gap store; he was granted instant credit after showing the store clerk his driver's license. In that case, LifeLock CEO Todd Davis admits, the fraud alert did not get set on the date it was requested. After requesting the alert a second time, our tester applied for another card and was asked to verify his identity more stringently. Davis adds that, either way, our tester would have been protected by LifeLock's service guarantee (see "The 'Million Dollar' Question," page 4).

In our in-store Debix test, the creditor verified our tester's identity by putting him on the phone with the store's credit department, bypassing Debix's automated system. According to Julie Ferguson, Debix's vice president of emerging technologies, "80 percent" of creditors call Debix to verify transactions—but they are not under any legal requirement to do so. Creditors can verify your identity in other ways, such as by sending a letter that asks you to mail them copies of W-2 statements, utility bills, or other documents.

In rare instances, creditors may issue credit without bothering to check your report. That seems to be what happened to Davis, who gained notoriety by publishing his Social Security number on LifeLock's home page and daring anyone to steal it. A Fort Worth, Texas, man promptly used Davis's identity to obtain a \$500 loan. Davis says that many low-amount lenders don't pull credit reports, which is why the Fort Worth creditor didn't see the fraud flag that LifeLock had placed on its CEO's credit report.

"This person would have been able to get the loan no matter what form of protection was in place," says Mike Prusinski, LifeLock's vice president of communications. "As soon as Todd was aware of the problem, he reported it to LifeLock—and the remediation services investigated, found the source of the identity theft, stopped additional attempts by this same person to buy cell phones and other goods, and prevented any other consequences from the identity theft such as damage to a credit score."

In February, Experian sued LifeLock, claiming that federal law prohibits corporations from setting fraud alerts for consumers, and calling LifeLock's marketing practices fraudulent.

"LifeLock claims it can prevent identity theft, but that's simply not true," says Experian spokesperson Rod Griffin. "By the time a credit report has been pulled, the person's identity has already been stolen. It gives people a false sense of security."

Davis says he can't comment on an active lawsuit but would "welcome the chance to work out a business solution [with Experian] that will continue to protect consumers."

Griffin won't say whether Experian will take legal action against other fraud-alert firms. TrustedID CEO Scott Mitic notes that the law allows consumers or their "personal representatives" to set flags, and says that his company has a good

DIY IDENTITY-THEFT PROTECTION:

A 12-Step Program

YOU DON'T HAVE to spend \$100 to \$200 a year to defend yourself from identity theft at the level of protection that a paid service offers. You can do almost everything the services do, for free. But following these steps will require time and effort.

1 Get a free copy of your credit report by visiting www.annualcreditreport.com. Don't be fooled by look-alike sites that promise free reports if you subscribe to their credit-monitoring services. Better yet, order by phone at 877/322-8228.

2 For DIY credit monitoring, order a free report every three months from a different bureau. Scan the report for unfamiliar information, such as accounts you don't remember opening.

3 Place a fraud alert on your credit report by calling one of the credit bureaus. (You can find contact information for all three bureaus by browsing to www.fightidentitytheft.com.)

4 Put a recurring event in your online calendar to remind you to renew your fraud alert in 90 days.

5 Tell the bureaus to stop selling your information to credit services, by calling 888/567-8688 or visiting OptOutPrescreen.com. Doing so will reduce but not eliminate the number of preapproved credit card offers you receive.

6 Request a free public records report from ChoicePoint (www.choicepoint.com). You'll have to print a

form and mail it, along with copies of your driver's license and proof of address. Scan the report for addresses and other details not related to you.

7 Take your name off other marketing lists by signing up for ProQuo.com's free service. In some instances, you may have to mail letters or navigate to a marketer's own site to complete your opt-out request.

8 Buy a mailbox that locks, or use a post office box. This will help prevent thieves from stealing your identity via paper mail.

9 Buy a crosscut paper shredder and shred junk mail to frustrate dumpster-diving identity thieves.

10 Never click a link from an e-mail message to log in to your bank or to any other financial institution. Type the secure site's address into your browser, bookmark it, and use that link to access your accounts. Otherwise, you risk having your identity stolen by phishers.

11 If you believe that you are a victim of identity theft, contact the Identity Theft Resource Center (www.idtheftcenter.org). Volunteers there can walk you through the process of restoring your identity.

12 Get educated. Mari Frank's Identity-Theft.org, the Privacy Rights Clearinghouse, and the FTC maintain huge libraries of information on how to avoid being victimized, and what to do if it has already happened.

relationship with the bureaus. Debix pays one bureau for the right to set flags, Ferguson says, but she declines to identify which one. As we went to press, Identity Guard announced that it would stop setting alerts for consumers “because Experian asked us to stop,” says Intersections’ Walston.

The ‘Million Dollar’ Question

Besides setting alerts, some services obtain your credit report and ask the bureaus to stop selling your info to credit card companies—two things you can do on your own (see “DIY Identity-Theft Protection,” page 3). Identity Guard and TrustedID will scan the Web and tell you if someone is trading your info online; but the odds of catching anyone are virtually nil, says Dmitri Alperovich, director of intelligence analysis for Secure Computing.

“This type of claim is mostly a gimmick,” he says. “You might find a few credit card numbers by searching the Net, but most of them aren’t lying around for public viewing, and the people who have them won’t deal with you unless you’re also a criminal.”

LifeLock, LoudSiren, and TrustedID provide million-dollar guarantees against identity-theft losses, but that promise comes with some strings attached; LifeLock says that it will hire specialists to contact lenders and law-enforcement agencies for you, and will pay other direct costs up to \$1 million. However, the guarantee doesn’t define which costs LifeLock considers “direct,” nor does it specify which costs are covered below the million-dollar cap.

TrustedID promises to pay the cost of reestablishing your identity, reimburse your legal fees, and restore up to \$5000 in lost income. LoudSiren covers theft losses, attorneys’ fees, and lost wages, with no cap. Debix’s \$25,000 policy covers expenses, attorneys’ fees, and up to \$2000 in lost wages.

But a million dollars is an inflated amount anyway. According to Javelin, the average out-of-pocket cost for identity theft victims in 2007 was \$691, and the average loss for people who had false accounts opened in their names was \$1066. Regardless, most victims of financial fraud don’t pay anything out of pocket because the financial institutions typically bear the costs, notes Rachel Kim, an associate analyst at Javelin.

TrustedID’s Mitic acknowledges the unlikelihood that anyone will need a million dollars of coverage. The real advantage, as he sees it, comes from having experts who can take the hassle and pain out of restoring customers’ identities.

“I think the biggest benefit customers get from TrustedID’s warranty is our restoration services—our commitment to hold a customer’s hand, do everything and anything they need to help them put their lives back together again,” Mitic says.

According to Prusinski, only 41 of LifeLock’s 840,000 subscribers have ever needed its restoration services. Mitic declines to release TrustedID’s customer numbers, but he estimates that 1 out of 10,000 need their identities restored. Debix’s Ferguson says that just 9 of its 300,000 subscribers have filed insurance claims; in most cases the theft had happened before the customer signed on to the service.

The Nuclear Option: Security Freeze

The third option beyond monitoring and alerts isn’t pretty.

“Rather than relying on fraud alerts or spending \$100 to \$180 a year on credit monitoring, consumers should consider a security freeze,” says Beth Givens, director of the Privacy Rights Clearinghouse. “Depending on how often you use it, a freeze can be an effective way to prevent identity theft and a lot cheaper than credit monitoring.”

With a freeze (which you can set up yourself for a small fee), credit bureaus won’t release your report at all—not ideal if you need to obtain a mortgage, change cable providers, apply for a job, or do anything requiring a credit check. Freezes are free for identity-theft victims in most states, Givens notes.

TrustedID can set up a freeze for you for \$15 plus any credit bureau fees, but you must mail it a power of attorney form. Or you can do it yourself via certified mail. The rules and fees vary depending on where you live, but the cost is usually \$10 per bureau. (Consumers Union has a guide to each state’s laws; see find.pcworld.com/60689.)

If after freezing your account you decide to change your cable plan or apply for a loan, you’ll probably have to pay \$10 per bureau to unfreeze your account for a specific creditor or a certain period of time. And because credit bureaus tend to move at glacial speed, you should make an unfreeze request long before you actually need it. Even with a freeze in place, identity thieves can use your medical insurance, ruin your eBay reputation, or apply for jobs with your name and résumé. Identity protection services can’t prevent such problems, says Linda Foley, director of the Identity Theft Resource Center and an identity-theft victim.

Identity protection services may help people who can’t be bothered to take the necessary precautions or who lack the resources to protect themselves. But you should choose carefully, read the fine print, and resist acting out of fear.

“I would say ‘Buyer, beware,’” says Foley. “There is nothing you can buy that will keep you from becoming a victim of identity theft—and if there was, I’d be the first in line to buy it.”

PC World Senior Editor Tim Moynihan and Senior Writer Tom Spring contributed to this story.



Joyce Carcaise • jcarcaise@intersections.com • 703.488.6100
www.identityguard.com