


[Threat Level](#)

Privacy, Crime and Security Online

# Lifelock Dinged \$12 Million for Deceptive Business Practices

By [Kim Zetter](#)  March 9, 2010 | 3:34 pm | Categories: [Crime](#), [Cybersecurity](#)

**Lifelock**  
Guarantee Your Good Name

Lifelock for People | Lifelock for Business | Our Guarantee | About Us | Enroll Now ▶ | 1 877 LI

**My name is Todd Davis**  
**This is my social security number 457-55-5462**

"I'm Todd Davis, CEO of Lifelock. Yes, that really is my social security number. No I'm not crazy. I'm just sure our system works. Just like we have with mine, Lifelock will make your personal information useless to a criminal. And it's **GUARANTEED.**"

Here at Lifelock, We Guarantee Your Good Name.  
No one else does because no one else can.

**More Testimonials:**

Stop Junk Mail. Stop Credit Offers.  
Stop Identity Theft. Guaranteed.

Enroll Now ▶

The CEO of Lifelock, Todd Davis, became famous for advertising his Social Security number on television ads and billboards promising his \$10 monthly service would protect consumers from identity theft.

The company also offered a \$1 million guarantee to compensate customers for losses incurred if they became a victim of identity theft after signing up for the service.

But the Federal Trade Commission said Tuesday that the [claims were bogus](#) (.pdf) and accused Lifelock, based in Arizona, of operating a scam and con operation. The commission announced, along with 35 state attorneys general, that it had levied a fine of \$12 million against the company for deceptive business practices and for failing to secure sensitive customer data. Of that amount, \$11 million will go to refund customers who subscribed to the service. Consumers will receive a letter from the FTC and their attorney general explaining how to take part in the settlement.

The FTC said that [Lifelock](#), which advertises itself as “#1 In Identity Theft Protection,” engaged in false

advertising by promising customers that if they signed up with its service their personal information would become useless to thieves.

“In truth, the protection they provided left such a large hole ... that you could drive that truck through it,” said FTC Chairman Jon Leibowitz, referring to a Lifelock TV ad showing a truck painted with the CEO’s Social Security number driving around city streets.

The company, he said, used scare tactics to convince potential customers they would be unprotected from identity theft without its service, and of warning them in letters that they were at a high risk of identity theft.

“I was a recipient of one letter,” Illinois Attorney General Lisa Madigan said.

For the annual subscription fee, Lifelock promised customers that it would place fraud alerts on their credit accounts with the three credit reporting agencies. As a result, the company said, thieves would not be able to open unauthorized credit or bank accounts in their name.

But Leibowitz said the promises were deceptive because thieves could still rack up unauthorized charges on existing accounts — the most common type of identity theft. It also couldn’t protect thieves from obtaining a loan in a Lifelock customer’s name.

In fact, [Lifelock CEO Davis was the victim of identity theft](#) in 2007 when a thief used his widely advertised Social Security number to obtain a \$500 loan in Davis’ name.

Lifelock also promised customers that sensitive data they provided the company to perform its protection services — such as their Social Security number, name and address and bank card information — would be encrypted and protected in other ways on Lifelock’s servers and accessed only by authorized employees on a need-to-know basis.

“Your documents, while in our care, will be treated as if they were cash,” the company promised.

In truth, the FTC said, until at least September 2007, the company failed to provide “reasonable and appropriate security to prevent unauthorized access to personal information stored on its corporate network” either in transit through the network, stored in a database or transmitted over the internet.

None of the data was encrypted, said the FTC, either in storage or in transit. The company also had poor password management practices for employees and vendors who accessed the information. Lifelock also failed to limit access to sensitive data to only those people who needed access.

What’s more, the company failed to apply critical security patches and updates to its network and “failed to employ sufficient measures” to detect and prevent unauthorized access to its network, “such as by installing antivirus or antispyware programs on computers used by employees to remotely access the network or regularly recording and reviewing activity on the network,” the complaint said.

The latter is particularly ironic. Lifelock often promoted its services to companies that experienced data breaches, convincing them to offer a complimentary Lifelock subscription to people whose data was compromised in a breach. All the while, the FTC claims, Lifelock was making its own customer information vulnerable to a breach.

“As a result of these practices, an unauthorized person could obtain access to personal information

stored on defendants' corporate network, in transit through defendants' corporate network or over the internet, or maintained in defendants' offices," according to the complaint.

According to the terms of an FTC settlement agreement with Lifelock to settle the allegations, the company must inform consumers about the limitations of its service. The company will also have to implement a data security program to protect the customer data it handles.

"As long as the company is honest and up front and lets consumers know what they're getting and has adequate security safeguards for customer information, we wish them well," said Leibowitz.

Lifelock said in a statement that, in October, it "rolled out the next generation of identity theft protection services that provide even better and broader protection to its valued members." The company added that its new-and-improved service, which was not the subject of the FCC inquiry, has prevented more than 5,000 fraudulent credit applications.

The company and its owners have been at the center of controversy for a number of years. According to an investigative report by the *Phoenix New Times* in 2007, Lifelock co-founder Robert Maynard Jr., was suspected at one time of being an identity thief himself and stealing his father's identity to obtain an American Express card. He had also been the target of another FTC investigation involving a previous business venture unrelated to Lifelock. Maynard [resigned from the company](#) after news of his past was published, but he continued to work for the firm as a contractor.

#### See also:

- [Lifelock Sued for Corporate Identity Theft](#)
- [Police Say Lifelock Founder Coerced Unusable Confession From Identity Thief](#)
- Lifelock Founder a Shady Identity Thief?
- [Lifelock Founder Resigns Amid Controversy](#)

Tags: [identity theft](#), [Lifelock](#), [Todd Davis](#)

[Post Comment](#) | [Permalink](#)

#### Also on Wired.com

- [Bottled Wind Could Be as Constant as Coal](#)
- [Funeral Flap: Justices Weigh Religion, Speech Rights](#)
- [The Wired Interview: FCC Chair Julius Genachowski on Broadband, Google and His iPhone](#)
- [DMCA Muscle Kills DVD Copying, for Real](#)
- [Flipping Off Cops Is Legal, Not Advised](#)
- [Facebook Patents Social Network Feeds, Raising Innovation Worries](#)

#### Related Topics:

- [U.S. Federal Trade Commission](#),
- [Consumer Protection](#),