

Identity Theft: It's Out of Your Hands

ARTICLE DATE: 02.11.09

By [Matthew D. Sarrel](#)

Have you noticed that along with copious stories about the state of the economy, you're seeing more and more reports of crimes large and small? I'm talking about everything from shoplifting to Madoff-caliber Ponzi schemes. Is it any wonder that **identity theft** is thriving? According to Gartner, 15 million identities per year are stolen, a new victim once every 2 seconds. Given 15 million a year, in ten years every U.S. citizen who uses the Net will have had his or her identity stolen. Well, either that or one unfortunate person will have to suffer through filing 150 million claims for himself. According to the [Identity Theft Resource Center](#), the incidence of identity theft increased by 50 percent in 2008 from 2007, and it continues to be one of the fastest-growing crimes in the United States. There is a thriving online international black market in stolen identities that local, state, federal, and international law enforcement seem powerless to stop. In fact, it has gotten so easy to steal and sell identities that prices have come down dramatically over the past two years. Why does it seem like it is getting easier for the bad guys and harder for the good guys like you and me? Because your identity is spread far and wide around the Internet, and its protection is out of your hands. A few months ago I wrote about how you can protect yourself from identity theft. Judging from the volume of reader responses, the steps that I provided have helped people not only recover their stolen identities but also prevent others from being stolen in the first place. Yet, protecting yourself is only part of the problem. How many entities on the Web and in the real world have you entrusted with some aspect of your identity? How many online retailers have your credit card info? **Corporate data** breaches are on the rise. The Identity Theft Resource Center's 2008 breach report reached 656 reported breaches at the end of 2008, reflecting an increase of 47 percent over last year's total of 446. In addition, ITRC estimates that only 2.4 percent of all the companies breached had encryption or other strong protection methods in use, while only 8.5 percent of reported breaches involved surmounting password protection. If a company can't even password-protect access to our identities, does it really deserve our business? Despite well-publicized thefts, business at companies that have been hit continues to thrive. Notification laws have proven thoroughly ineffective at *preventing data* breaches. Not only that, the next time you receive a notification letter—and odds are you will—read it carefully. Not a single one of the 50 or so letters that readers have forwarded to me mentioned concrete actions that the companies were going to take to prevent it from happening *again*. If that doesn't indicate how valuable they consider the safety of your identity, then I don't know what does! —next: Mugged by Merchants? >

Mugged by Merchants?

The point is that you can do everything to protect your valuable identity—and you will, because it's yours and you care—but after your info enters the ether, there are gaping holes in the protection of your identity. The holes are called online retailers, banks, mortgage providers, ski resorts, hospitals, and even the government. And guess what? They care a hell of a lot less about protecting your identity than you do. It's time for that to change, and it will happen only when we hit them where it hurts, in the bottom line. The next time an entity allows your identity to be stolen, cancel or transfer your account. Don't shop there again. If you got mugged in a physical store, would you keep shopping there? What to do when you are victimized by a data breach:

1. Close your account. Send an [e-mail](#) explaining why and demand confirmation that your confidential information has been deleted from their system. If you can't simply close your account, as in the case of a bank or mortgage, transfer it to another provider. Make your original provider waive all cancellation fees and pay for the transfer. Unwilling to close the account? At the very least, have all related account numbers changed.
2. Cancel all affected credit and debit cards.
3. If the breached entity is the government, write to your local, state, or federal elected officials to make them aware of your displeasure.
4. Immediately call all three credit bureaus ([Equifax](#), [Experian](#), [TransUnion](#)) to place a fraud alert on your accounts and request free credit reports to review carefully.
5. Demand [identity protection](#) services from the breached entity.
6. Inspect all account statements on arrival.
7. Inform all friends, relatives, and acquaintances of the breach and encourage them to avoid the breached entity.

[Copyright \(c\) 2009Ziff Davis Media Inc. All Rights Reserved.](#)