

Coming soon from Random House: "The GigaLaw Guide to Intern



One of Yahoo's "most popular" sites!

Contents:

[Home](#)
[News](#)
[Discussion List](#)
[Bookshelf](#)
[Poll](#)
[GigaLaw-to-Go](#)
[Store](#)
[About Us](#)
[Contact Us](#)

Search

[Search Tips](#)

New & Noteworthy:



[Why the Entertainment Industry's Copyright Fight is Futile](#)
 By Peter Yu

GigaLaw.com®: "Legal Information for Internet Professionals"

Identity Theft: What It Is and How to Protect Against It

By Harry A. Valetk

Summary: Identity theft is the fastest-growing white-collar crime in the United States, affecting more than 600,000 Americans in 2001. Unfortunately, there is a gaping hole under existing law for preventing identity theft schemes. This article explains the scope of identity theft and its financial impact and offers some practical "do's and don'ts" for avoiding problems.

Author: The author of this article, Harry A. Valetk, is an attorney for the Social Security Administration in New York. He is licensed to practice law in the state of New York. The opinions expressed in this article belong to the author, and are not those of the Administration. E-mail: legaleagles@cyberlawenforcement.com



Introduction

Would you be surprised to learn that someone could easily steal your identity simply by accessing your Social Security Number (SSN)? Armed only with this unique nine-digit number, a thief would then have free reign to ruin your good credit, prevent you from getting work, stop you from refinancing your home, or even use your good name to commit a crime.

Shocked? Well, then, you may be even more disheartened to learn that identity theft is the fastest-growing white-collar crime in the United States, affecting more than 600,000 Americans in 2001. In that year alone, ID thieves stole nearly \$100 million from financial institutions, or an average of \$6,767 per victim, [according to](#) the Federal Trade Commission (FTC). About 13% of all ID theft victims reported out-of-pocket expenses to remedy their credit problems, spending a collective \$13 million on legal and notary fees, or roughly \$1,173 per person.

On top of the financial burdens, officials estimate that ID theft victims spend an average of 175 to 200 hours to repair the damage

Augu

- Web I
Indicted
Qaida Te
- Senal
Internet
Campaig
- Micro
Progress
Consent
- AT&T
Providing
Some Ar
- Judge
to Dismi:
Hyperlin
- Electr
Used in C
Convictic

Rea

e-mail

S

SEE ALSO

[What Companies and Individuals Can Do to Protect Privacy in the Internet Age](#)

[Tips and Tricks for Maintaining Your Privacy Online](#)

[Facts About Privacy and Cyberspace](#)



[Pater
Esse](#)
Alan L.
New \$€

[Law](#)
Leonar

[Pater
to Ge](#)
U. S. D

[Intelle
Prope](#)
Arthur I

[Remt
Attic](#)
Kevin C



[Are Pop-Up Advertisements on the Web Illegal?](#)
By Doug Isenberg

[Making Your \(Trade\)Mark on the World](#)

[Antitrust Scrutiny of Business-to-Business Web Sites](#)

done by ID thieves. As one victim put it in a [consumer complaint](#) to the FTC, "Someone used my Social Security Number to get credit in my name. This has caused a lot of problems. I have been turned down for jobs, credit and refinancing. This is stressful and embarrassing. I want to open my own business, but it may be impossible with this unresolved problem hanging over my head."

[Copy](#)
[Copy](#)
Siva V
[Getir](#)
[Perm](#)
Richar
(Price
Prive

How Bad Is It?

Describing the daunting task to a congressional subcommittee in 2001, New York City Police Detective Michael Fabozzi, an expert in ID theft crimes, pointed out that the present system is not just vulnerable, but it also leaves victims to fend for themselves trying to clear their credit history and good names. For others unfortunate enough to fall victim to "criminal identity theft," in which a perpetrator uses a stolen identity on arrest, they soon learn how difficult it can be to expunge criminal records.

At the heart of the ID theft crisis is the fact that the SSN has become the de facto national identifier. Originally, the SSN was created in 1936 solely for tracking workers' Social Security earnings records. By sharp contrast, today the SSN has been described by U.S. News & World Report as "the magic nine-digit number that unlocks doors and is the password to identity theft."

So Who's Vulnerable?

Given its unfettered power -- combined with our single, unique-identifier dependency -- the SSN is a valuable asset that is too often subject to abuse. And, unfortunately, the risks continue to grow even among the most wary consumers.

Take, for example, a Maryland resident who fell victim to ID theft, despite her precautionary practice of shredding sensitive financial statements and reviewing her credit report annually. In her case, her identity predator worked for a business that maintained HMO databases and was able to access her SSN and date of birth. Using only these two pieces of information, the perpetrator obtained more than \$36,000 in goods while adversely affecting the victim's ability to refinance her home and obtain credit.

Another case involved one of the authors of Pennsylvania's anti-ID theft law. In fact, just weeks after Pennsylvania made ID theft a crime in 2001, Rep. Matthew Baker reportedly discovered that someone had stolen his identity.

What About Existing Law?

From a legislative perspective, one of the main problems is that no federal law governs -- or even limits -- the use or disclosure of someone's SSN among private entities. This leaves private companies free to deny anyone credit, service or membership for refusing to furnish a SSN. Simultaneously, and contrary to popular belief, the Social Security Administration has no power to control

how private entities use their account numbers.

The result is an extremely vulnerable system that puts all the burden on the consumer. With no power to control how their SSN is kept, used or distributed, many are left simply to sit and wait for an ID thief to strike.

Unfortunately, there is a gaping hole under existing law for preventing ID theft schemes. Although fraudulently using an individual's identity information is a crime, the after-the-fact approach currently in place does little to protect consumers from identity theft before it occurs.

In November 2001, consumers suffered another blow when the U.S. Supreme Court put the burden on them to routinely check their credit reports or find themselves unable to sue negligent credit-reporting agencies. The case involved a patient who fell victim to identity theft after her doctor's former receptionist stole her SSN from an intake form and opened several credit accounts. In reversing the U.S. Court of Appeals for the Ninth Circuit's decision, the [Supreme Court held](#) that the two-year statute of limitations to bring an action under the Fair Credit Reporting Act begins when the alleged wrongful disclosure occurred, not when an individual discovered the wrongful disclosure.

Pending Legislation May Help

To address the ever-escalating ID theft crisis, federal legislators proposed about 10 bills in 2001 intended to protect consumers from SSN misuse. Although none was actually passed, consumer advocates believe the tragic events of September 11 have raised a new awareness about our existing vulnerabilities.

Not surprisingly, the proposed bills varied widely in scope, trying to balance consumer protection with corporate efficiency. Some bills represented compromises for the competing interests sought by consumers and businesses by simply prohibiting private entities from the selling, purchasing or displaying of SSN information. Others went even further by penalizing any entity that would deny goods or services to any individual that refused to furnish his or her SSN.

To be effective, however, new legislation addressing ID theft must give consumers control over their SSNs. It should be simple, based on fair information practices and include few exceptions or loopholes. At the same time, any new law should build on -- not weaken or overlap with -- existing privacy protections, including those of the Privacy Act or the [Gramm-Leach-Bliley Financial Privacy Act](#). Above all, it should limit SSN use to only those purposes that benefit the number holders, not information brokers, mass marketers or other entrepreneurs that carelessly expose it to abuse by making it available for a fee.

How Can I Protect Myself? Do's & Don'ts

In the meantime, you should consider the following "do's" and "don'ts" to protect yourself from ID theft:

- Do ask how your SSN or other personally identifiable information will be used before revealing it to anyone.
- Do be sure to cross-shred every document containing identifying information. By simply tearing these documents in half, you will likely leave important information plainly visible to a predator's eye.
- Do be sure to get a copy of your credit report at least twice a year. For extra protection, consider signing up for a credit monitoring service from a company such as Equifax.
- Do call (888) 567-8688 to stop those pesky pre-approved credit card offers.
- Do pay attention to your billing cycles, and guard your mail from thieves. If you're planning an extended trip away from home, call the Postal Service's vacation hold number at (800) 275-8777.
- Don't reveal your SSN unless absolutely necessary.
- Don't carry rarely used credit cards or any unnecessary identification that would give an ID thief access to sensitive confirmatory information (such as your mother's maiden name, an old address, etc.).
- Don't be fooled. ID thieves are not always strangers; sometimes they turn out to be a coworker, acquaintance, ex-lover or even a relative.
- Don't give out personal information over the phone, through the mail, or post anything on the Internet. ID thieves often pose as legitimate businesses to get to your sensitive information.

-
- This article was originally published on GigaLaw.com in April 2002

[Terms and Conditions](#) | [Privacy Policy](#)

Copyright © 2000-2002 Dolesco LLC | [Douglas M. Isenberg, Esq.](#), Editor & Publisher

