

# Richmond Times-Dispatch

OPINION: | [Editorials](#) | [Letters](#) | [Commentary](#)

Sunday, August 30, 2009 |

[Midlothian, VA](#) 79° Feels Like: 79° Mostly Cloudy

## Social Security numbers facilitate identity theft



Text size: [small](#) / [medium](#) / [large](#)

By [IRIS TAYLOR](#)

Published: August 30, 2009

A happy family vacation in Virginia Beach turned into a nightmare for a retired Chesterfield County couple who became victims of identity theft.

Two days after Robert and Doris Struhmer's trip, someone began draining \$5,200 from their checking account.

Over a 10-day period, unknown to them, a thief conducted numerous fraudulent transactions by phone and with fake checks using the Struhmers' checking account and routing numbers, even paying telephone and cell-phone bills and making a mortgage payment.

### MORE

- [Social Security numbers facilitate identity theft](#)
- [No one is immune to identity theft](#)

### RESOURCES

- Social Security Administration: (800) 772-1213
- Social Security office in Midlothian: (804) 744-0227

The losses came to Struhmer's attention when he received a call from Philadelphia police informing him that a man had been arrested with Struhmer's name, address and Social Security number in his possession.

Today, the Midlothian retirees are still scratching their heads about how it happened.

They've gotten their money back, closed the compromised accounts and put alerts on their credit reports. But they face traveling to Philadelphia next month to testify in court against the criminal.

"It has been a total nightmare," Struhmer said. "You're just waiting for something else to happen."

Martha Sharp, another area resident, said two banks, plus a former employer and possibly the state of Virginia, over the past several years failed to protect her Social Security number and a lot of other sensitive data from being stolen or lost.

"This is the world we live in now," she said. "I guess all these entities have a right to my Social Security number but are apparently unable control their systems to maintain an individual's privacy."

Sharp is correct.

Many businesses, government agencies and other entities are legally entitled to consumers' Social Security numbers.

Others, though, are not. The problem is those not entitled still ask, consumers tell, data slip out from databases, and con artists ply their trade, ripping off people's identities both from businesses and consumers.

So, which entities are entitled to know consumers' Social Security numbers? Which are not? What recourse is there for people who don't want to disclose their number? Why is it so critical to protect Social Security numbers now?

...

In a December report, "Security in Numbers: SSNs and ID Theft," the Federal Trade Commission said identity theft "continues to be a major problem in this country," with victims numbering in the millions each year and out-of-pocket losses in the billions of dollars.

Social Security numbers play a major role in facilitating identity theft. Because private and public-sector entities have

- Federal Trade Commission identity-theft hot line: (877) 438-4338
- Equifax: (800) 525-6285
- TransUnion: (800) 680-7289
- Experian: (888) 397-3742

### **IT'S MORE THAN A NUMBER**

With your Social Security number, a thief masquerading as you can:

- open new credit accounts;
  - gain access to existing accounts;
  - commit medical identity theft;
  - get a job;
  - obtain government benefits; and
  - get a loan.
- Crooks can steal your SSN by:
- hacking into a computer that has your number on it;
  - sending phishing e-mails to trick you into revealing your number;
  - stealing the number that you provided to an unsecured Web site;
  - buying your number on the black market (going rate: 90 cents to \$25 each);
  - secretly using malware encoded to scoop up your data;
  - using spyware to collect the number from your computer;
  - using keystroke loggers to capture what you type;
  - diving into garbage cans and stealing discarded information;
  - stealing workplace records;
  - stealing your mail;
  - stealing your wallet or purse;
  - accessing public records containing SSNs; and
  - calling and pretending to be an institution, then tricking you into disclosing personal data.

**Source: Federal Trade Commission**

used them so extensively as an identifier, "the SSN has become both available and valuable to identity thieves," the FTC said.

That's why it is critical for consumers to limit access to their Social Security numbers. But some are losing the battle.

The Office of Inspector General said it received more than 14,200 allegations of Social Security number fraud or misuse in 2008, versus 12,200 in fiscal 2007. It opened more than 700 fraud cases related to Social Security numbers in 2008, spokesman George Penn said.

Consumer Jean Johnson of Highland Springs wants to know why some businesses like telephone companies ask for people's Social Security numbers.

"It makes me feel very vulnerable," Johnson said. "I'm very protective of my Social Security number."

Social Security Administration spokeswoman Dorothy Clark said if a business or government agency is not on its list of entities legally entitled to have consumers' numbers, "you're not legally required to give that number."

On the list: the Internal Revenue Service, various federal and state government agencies and departments, banks, employers and agencies that administer government programs.

Not on the list: doctors' offices and retailers.

Bon Air resident Beverly McNeer wonders whether businesses that are not entitled to your Social Security number can deny services or products if you do not produce it for them.

Clark says they can. "If you refuse to give them your Social Security number, you may not get the service you're trying to obtain."

It's a consumer's decision whether to give up their Social Security number or walk away and do business elsewhere, she said.

That can be disheartening if a person wants, say, a new doctor, but that doctor's front office requires providing a Social Security number.

A consumer can ask the company to use a different identifying number instead of a Social Security number, suggested Beth Givens, director of the Privacy Rights Clearinghouse in San Diego.

## **PROTECT YOUR SSN**

These are some practices to help guard against identity theft:

- Shred documents with personal data on them before discarding.
- Remove personal data such as your income-tax return from your computer hard drive.
- Never respond to e-mail from a stranger asking for personal information.
- Do not download free music or videos because that may allow crooks to snoop into personal data on your computer.
- Monitor your credit reports quarterly for free at [AnnualCreditReport.com](http://AnnualCreditReport.com) or (877) 322-8228.
- Get your SSN removed from ID cards if possible.
- Place a fraud alert on your credit reports so that no one can apply for credit without you being contacted.
- Check your Social Security statements to see that no one's working using your number.
- File a police report if your SSN is stolen.
- Place a security freeze on your credit reports so that no stranger can access your credit history.
- Ask businesses that request your SSN to assign a different account identifier, such as your driver's license number.
- Don't carry your Social Security card in your wallet unless specifically needed.
- Don't carry your Medicare or Medicaid card, especially if your medical providers have previously copied it.
- If you feel uncomfortable without the card, make a copy

"What we recommend is that individuals offer to give their driver's license number instead," she said.

Can consumers compel an entity to stop using their Social Security number?

"You could say it to them, but they don't necessarily have to comply," said Naomi Lefkowitz, an attorney in the FTC's division of privacy and identity protection. "There's nothing to legally stop them from using it as an identifier.

"There are a number of companies that are moving away from using Social Security numbers as authenticators and additionally as internal identifiers," she said. But "there are other companies who aren't doing a thing. It can be a costly and time-consuming process, depending on their system."

The federal Medicare/Medicaid system still uses consumers' Social Security numbers on identification cards.

"The transition to [a] new Medicare identifier would cost more than half a billion dollars," said Tony Salters, spokesman for the Centers for Medicare & Medicaid Services. It would take more than three years "and result in enormous upset to our beneficiaries, more than a third of whom have had the same identifier for at least a decade."

Hopewell resident G. Lee said: "It is difficult to protect your Social Security number, especially when you are required to show your Medicare card when you need medical care, making it necessary to carry it at all times."

That may not be necessary, said Kim Brundage, spokeswoman for the Bon Secours Richmond Health System.

Even if a patient arrives unconscious, "the emergency department would seek identification like a driver's license and would use that information to obtain their Medicare/Medicaid status," she said.

Many companies and organizations have succeeded in safeguarding consumers' data. But others, among them some of the most trusted entities in the nation with deep pockets and sophisticated layers of security, have utterly failed to protect consumers' data, according to the Privacy Rights Clearinghouse.

The clearinghouse, which tracks data breaches, reported that more than 263 million records containing sensitive personal information, such as Social Security numbers, were involved in security breaches in the U.S. since January 2005.

"You should never assume that your Social Security number is being held securely," Givens said. "There are many factors outside the control of that company, such as hacking and dishonest employees."

Consumers often have little recourse when a company lets a person's sensitive data slip out of its database, she said.

of the original and put it away, then blacken the first five numbers on the copy and cut it to size.

**Source:** Privacy Rights Clearinghouse, Social Security Administration, LifeLock Inc., Metro Richmond Identity Theft Task Force, IdentityTheft.org, Consumers Union

"Several individuals have attempted to sue companies that have data breaches. But they have not been successful. If there's no evidence that a data breach resulted in ID theft, it's very difficult to sue," she said.

While many companies that have had a data breach offer free credit monitoring to those affected, others don't.

Many companies don't even offer free credit monitoring to the consumers whose data they let slip away. "There is no law that says that they must provide you any credit monitoring," said Mari Frank, a California ID theft and privacy attorney. "At least, there's no federal law."

SunTrust Banks Inc., with \$179 billion in assets, would not explain why it uses customers' Social Security numbers as an identifier, if it intends to stop using them that way and if there's a prohibitive cost involved in switching to another type of identifier.

SunTrust spokesman Hugh Suhr said only: "Protecting the confidential information of our clients is paramount, and we incorporate extensive measures within our operations to help safeguard that information."

Many consumers fear their Social Security numbers have been so compromised over time that trying to protect them is like attempting to get toothpaste back in the tube.

Sharp noted: "I have had no known credit trouble yet, but still feel I'm sitting on a disaster waiting to happen."

---

Contact Iris Taylor at (804) 649-6349 or [itaylor@timesdispatch.com](mailto:itaylor@timesdispatch.com).

## Reader Reactions

Posted by ( David ) on August 30, 2009 at 7:45 pm

The problem with playing with the SSN is this. If you are applying for credit and you've "played" with giving out SSNs with "typos", it's very likely that the credit report pulled by the prospective credit grantor will contain the real SSN and the "typo" SSNs as well, along with any pertinent warnings regarding the SSNs (like account holder reported deceased, number not issued, date in which the number was issued[important if you're 32 and using a SSN issued in the 1950's]).

The credit report will tie them together - basically saying, "Hey, there's also another Joe Smith at 123 Main Street with a different SSN".

Now you've raised a red flag or at least a warning flag to the potential credit grantor that more investigation is needed, perhaps they'll just reject your application straight out because of unverifiable information. More hassle for you, but you can decide if it's worth it.

### Report Inappropriate Comment

Posted by ( anonymous ) on August 30, 2009 at 12:19 pm

binary1com:

I think that you may be missing the point. Obviously no one (an honest person) is going to give the wrong social security number when applying for credit. 0001, 0011, 0111, 1111 may be correct, but the real world is a lot more complicated. Common sense applies here.

Report Inappropriate Comment

Posted by ( binary1com ) on August 30, 2009 at 11:50 am

J-Reb—while this may seem like a great idea.. here's why it will harm more than help:

- 1) If you pick the "random" SSN of a deadbeat, you may get less favorable terms, pay higher prices or be denied services. Even if the "random" SSN is "on time payer" when applied, what happens if they go bankrupt?
- 2) Do you really want to take the chance of "mixing your credit" with another person—the damage is very hard to correct. You have nothing to gain, only something to lose.

You're just inconveniencing yourself and the businesses that are trying to serve you with ZERO gain.

I'm working on a project for a client with a database containing SSN's for 10 million customers, I don't have \*ALL\* the details needed to steal their identities, but I have enough for a "good start"—As long as dishonest people exist in this world, there will be identity theft, it just so happens that credit agencies make it TOO EASY right now.

The reason a lot of doctors offices REQUIRE that you give a SSN is because when they perform 3rd-party billing, a lot of the "other agencies" use the SSN to find your account.

If you want to pay 'cash' for everything at a doctors office, I'm sure they will bend the rules. Otherwise, just play along—If someone wants to steal your identity, they will, there's nothing you can do about it.

Checking your banking statements and credit reports regularly (everyone gets 3 free reports per year, check one agency every 4 months) is the best thing you can do.

Keeping your SSN hidden from a doctors office or the phone company just makes it harder for you and the vendor.

Report Inappropriate Comment

Posted by ( anonymous ) on August 30, 2009 at 11:47 am

J-Reb:

If a merchant or someone is demanding my social security number for no valid reason, I have been transposing numbers for years without any consequences. I am not attempting to defraud anyone. If I cannot justify giving out my phone number, I supply the number for local weather. A few years ago I used 'Dial A Prayer' number or TIGER11 for the time. An honest person has to be so careful these days with any personal information. Paying \$12.99 per month for credit monitoring and keeping a close eye on the bank balance also offers a little peace of mind. However there are no guarantees that it will not happen to the most vigilant person.

Report Inappropriate Comment

Posted by ( J-Reb ) on August 30, 2009 at 9:44 am

David, you definitely raise some good points although I think you're a bit too worried about those possibilities and maybe not worried enough about what happens when too many people have your *correct* SSN!

Meanwhile, without wanting to disclose too much about my technique, I'll add that 1) I hardly ever have to do it and 2) I choose numbers which look like typos. Get it? So the 'mistake' might well appear to have been someone else's, somewhere else along the miserable chain of data mining. I'm innocent, honest ;)

[Report Inappropriate Comment](#)

Posted by ( revnhøj ) on August 30, 2009 at 8:43 am

Unfortunately adding a fraud alert to your credit report presents a whole new set of problems. I added one to Experian and it's impossible to remove without - get this - sending all my personal information \*including my social security number\* in the clear through the mail. If this isn't done I cannot get any credit.

We really need to shut down these credit reporting agency monopolies. I never gave them permission to collect my personal information - did you?

[Report Inappropriate Comment](#)

Posted by ( David ) on August 30, 2009 at 7:04 am

j-reb, doing the "change a number" thing may work for a while, but it's not a generally good idea.

If you change the wrong digit, you'll end up giving a SSN that's either not valid (either unissued or one that couldn't possibly be yours because of the way the numbers are issued), or worse, one that's valid that belongs to someone else.

What happens next is that your credit report will get flagged because it looks like you're using two numbers or an invalid number. Perhaps worse is that your name can get associated with the address of the person who really owns the SSN and that person may well begin getting mail addressed to you at their address - maybe even preapproved credit offers.

In short, you can open yourself to allegations of fraud and even possibly aid an identity thief.

[Report Inappropriate Comment](#)

Posted by ( J-Reb ) on August 30, 2009 at 12:30 am

Bon Air resident Beverly McNeer wonders whether businesses that are not entitled to your Social Security number can deny services or products if you do not produce it for them.

Clark says they can. "If you refuse to give them your Social Security number, you may not get the service you're trying to obtain."

Like telephone or electrical service to your house, for instance. Are you supposed to do without?

My advice (as someone who's had his identity stolen): make a slight error in the number when giving it to businesses who demand it but have no right to it. No harm, no foul, and it gets you past the bored functionary making the demand because they're required to. It works :)

[Report Inappropriate Comment](#)

Page 1 of 1