

GRACE – ASK SAVA ID Theft Protection June 1, 2011

ASK SAVA: I hear about Identity Theft every day from someone, from losing their credit card to concerns about their medical records.

Q – Everyone needs to understand the basics of identity theft. If you have a television and actually get a channel that broadcasts news once or twice a day, it's a pretty good bet that you've heard about identity theft. For that matter, a television isn't a necessary requirement to know that identity theft exists. People talk about it every day. But what exactly is identity theft?

Identity theft is often confused with other crimes that lead to identity theft. As an example, a thief caught stealing credit card numbers isn't necessarily committing identity theft. He's committing a financial crime. Identity theft happens when a criminal steals your personal information for the express purpose of pretending to be you.

Why would anyone want to be you? What an identity thief wants from you isn't really your life; it's just everything that tells others that your life belongs to you. Your Social Security number is one good example. A person who can't get a Social Security number will sometimes steal one that belongs to someone else, so they can have the benefits of having a Social Security number.

Another reason that identities are stolen is to gain access to your financial accounts. In fact, this is one of the most common reasons that a criminal is trying to become you. Your power lies in your good name, and if a thief can gain control of your good name, then they also control that power.

The power that we mean is purchasing power. The ability to own a home, hold a job, and apply for credit. These are what identity thieves are after.

Above all else, identity theft is a crime of opportunity. A criminal, or even someone who is not yet a criminal, sees an opportunity, and takes advantage of it. Even criminals who work as part of identity theft rings depend on opportunity to gain access to the information they need.

In fact, you might be surprised to learn that the majority of identity theft doesn't happen online. More identity theft takes place in the 'real world' than online. And it often happens in ways that you would never expect.

One of the most common methods of identity theft is dumpster diving. Dumpster diving is when someone goes through your trash looking for identifying information. And you don't have to use a dumpster. The trash can that you put out at the corner the night before pickup is just as

vulnerable as a public dumpster.

Many other threats exist in the real world, too. Shoulder surfing is one that might surprise you. When a criminal is shoulder surfing, they're watching over your shoulder, waiting to capture your personal information when you're most unaware. Many people put themselves at risk using a cell phone. A shoulder surfer will snap pictures or capture video of buttons that you key in while you're using the phone.

Protect Yourself

It's so difficult to know who might be an identity thief, where they might strike, or what method they may use to capture your personal information that you must always be vigilant about protecting yourself. In public and even in your own home you need to develop safe living practices that help you protect yourself.

The most important safety practice you can develop is to always be vigilant about your surroundings and the risk that you create for yourself. Think about the ways that you could be compromising your information – throwing out junk mail, leaving your mail in the mailbox for days at a time, and using your phone for credit card purchases while you're standing in line at the grocery store. And then change those habits.

Only by being aware of the risks that are associated with identity theft, and being conscious of how you contribute to those risks can you begin to protect yourself. As the old adage goes, "knowing is half the battle."

Types of ID Theft

There are several "types" of ID theft. Each one affects certain areas of our lives, and has specific things to keep in mind when trying to deal with it.

- **Financial Identity Theft**
- **Medical Identity Theft**
- **Criminal Identity Theft**
- **Driver's License Identity Theft**
- **Social Security Identity Theft**

- **Synthetic Identity Theft**
- **Child Identity Theft**

Where to Find Help

It's critical to get in contact with the right people quickly. Some of the people you'll need to talk with you probably already know – your local bank manager, your local police department, etc.

There are two key rules to remember as you work with your situation: keep the originals of all paperwork, and document everything you do.

The Federal Trade Commission's identity theft site has links to the **identity theft affidavit** – a vital document as you work to restore your identity. You can also call the FTC at 877-ID-THEFT (877-438-4338).

<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

The **Identity Theft Assistance Center (ITAC)** has also put together some [frequently used fraud hotlines](#) (including investment companies.)

<http://www.identitytheftassistance.org/pageview.php?cateid=62>

Place a fraud alert with one of the three primary credit reporting agencies. It will automatically be sent to the other two, and remain in effect for 3 months.

- Experian – 888-397-3742 (TDD 800-972-0322)
- Equifax – 888-766-0008 (TDD 800-255-0056)
- Transunion – 800-680-7289 (TDD 877-553-7803)

Talk to the check verification companies if your bank account has been compromised, a new bank account set up in your name, or you find out bad checks were written on your account.

- CheckRite – 800-766-2748
- ChexSystems – 800-428-9623
- CrossCheck – 800-552-1900
- Equifax – 800-437-5120
- National Processing Company (NPC) – 800-526-5380
- SCAN – 800-262-7771
- TeleCheck – 800-710-9898

The [U.S. Secret Service](#) also has a hand in the investigation of crimes associated with financial institutions.

<http://www.secretservice.gov/faq.shtml>

Look at the [Internal Revenue Service](#) website for information on dealing with tax-related identity theft, such as a bogus return filed in your name.

<http://www.irs.gov/privacy/article/0,,id=186436,00.html>

The [Social Security Administration's identity theft site](#) answers some questions on lost social security cards and misused numbers.

<http://www.socialsecurity.gov/pubs/10064.html>

File a complaint with the [U.S. Postal Inspection Service](https://postalinspectors.uspis.gov/forms/IDTheft.aspx) if you believe your mail has been diverted, or that someone is tampering with your mail.
<https://postalinspectors.uspis.gov/forms/IDTheft.aspx>

File a report with the [Internet Crime Complaint Center \(IC3\)](http://www.ic3.gov/default.aspx) if you believe your identity was compromised due to internet activity (a Trojan horse, virus, malicious website etc.)
<http://www.ic3.gov/default.aspx>

The [U.S. Department of Justice](http://www.justice.gov/criminal/fraud/websites/idtheft.html) has a site as well, although they will most often refer you to a more-appropriate resource.
<http://www.justice.gov/criminal/fraud/websites/idtheft.html>

The [National Conference of State Legislatures](http://www.ncsl.org/IssuesResearch/BankingInsuranceFinancialServices/IdentityTheftStateStatutes/tabid/12538/Default.aspx) has a [reference guide](http://www.ncsl.org/IssuesResearch/BankingInsuranceFinancialServices/IdentityTheftStateStatutes/tabid/12538/Default.aspx) for various identity theft related state laws. This information will probably come in handy.
<http://www.ncsl.org/IssuesResearch/BankingInsuranceFinancialServices/IdentityTheftStateStatutes/tabid/12538/Default.aspx>

For legal issues, you'll want to get in touch with your [State Bar Associations](http://www.naag.org/). You may also want to get in touch with your state's Attorney General – you can find his/her contact information on the [National Association of Attorney's General website](http://www.naag.org/).
<http://www.naag.org/>

Contact the CT Department of Motor Vehicles at
<http://www.ct.gov/dmv/site/default.asp>

Contact the RI Department of Motor Vehicles at
<http://www.dmv.ri.gov/>

Medical identity theft is a special situation, and will require more attention to little details. Although you will still want your credit report, the [medical identity theft](#) resources page will also give you additional information you will need when dealing with healthcare providers...especially since the new [HITECH](#) law has been adopted. You may find yourself also needing to get in touch with your [state insurance commissioner](#).

- [Connecticut \(203\)297-3800](#)

- [Rhode Island \(401\)277-2223](#)

Identity Theft Assistance Sites

These sites may provide additional information. As always, if you have a resource you think should be on this page, let your guide know with a link in a quick email.

The **Identity Theft Resource Center** has compiled a [very helpful map](http://www.idtheftcenter.org/map.html) to identify local assistance.

<http://www.idtheftcenter.org/map.html>

The [Privacy Rights Clearinghouse](http://www.privacyrights.org/) is a valuable resource for tracking data breaches as well as general information about recovering your identity.

<http://www.privacyrights.org/>

