

Introduction to Identity

Types of Identity 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: When people hear the words "identity theft" they usually think of credit reports and bank accounts. We hear about data breaches like TJ Maxx ([47.5 million credit cards](#)) and Heartland Payment Systems (130 million credit cards) regularly. Our faith in our financial institutions is shaken. Some of us are thinking about keeping our money in the mattress again.

Medical Identity Theft: The World Health Organization said this is "the information crime that can kill you." ([Read the full publication here \(PDF\).](#)) It's not just the most dangerous form of identity theft, it's also one of the hardest to fix. If you're a victim of medical ID theft, you have your work cut out for you.

Criminal Identity Theft: This one may be as bad as medical ID theft. The easiest way to find out if this has happened to you is to get caught speeding. The officer who stops you will run your license and registration. If there are warrants out for your arrest, s/he will give you a pretty set of matching silver bracelets, and free public transportation.

Driver's License Identity Theft: This may be the easiest form of ID theft to commit. Your purse/wallet gets stolen, and your driver's license gets sold to someone who looks like you. Then it's easy for them to get other forms of ID in your name. This type of ID theft spreads to others, especially criminal identity theft.

Social Security Identity Theft: There are millions of people working in America who don't want to pay taxes. It may be an illegal immigrant, a deadbeat parent, or a paroled criminal trying to shake their past. Your SSN may be the most valuable piece of personal information a thief can steal.

While the Social Security Administration isn't required to tell you about all these jobs, the IRS will want you to pay the taxes. This can be a tough battle, too. For a non-government agency, the IRS has unbelievable power. Expect a lot of hoops to jump through here. Although it's gotten easier over the past few years, the process is still time consuming.

Synthetic Identity Theft: This is the "latest thing" in the ID theft world. The thief will take parts of information from many victims and combine it. The new identity isn't any specific person, but all the victims can be affected when it's used. It will show up in the areas above, so look to those sections for additional information.

Synthetic identity theft has also been used to describe any act in which the criminal attempts to convince someone they are another person, real or fictional. This careful wording is no doubt reactionary to the [the US Supreme Court ruling that an illegal immigrant has not committed a crime](#) unless he/she knew they SSN they were using belonged to an actual citizen.

Child Identity Theft: When dealing with your own identity theft, be sure to look into your children's. Our kids are a big target for ID theft. An 8-year-old won't be looking at their credit for at least eight more years, probably longer. Sadly, the thief in these cases is almost always a family member or close friend. This means the parents will usually not want to press charges, and the ID thief counts on that.

Fair Information Practice Principles

Transparency: Organizations should be transparent and provide notice to the individual regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).

Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII.

Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.

Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

Rooted in the United States Department of Health, Education and Welfare's seminal 1973 report entitled *Records, Computers and the Rights of Citizens* (1973), these principles are at the core of the Privacy Act of 1974 and are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. A number of private and not-for-profit organizations have also incorporated these principles into their privacy policies.