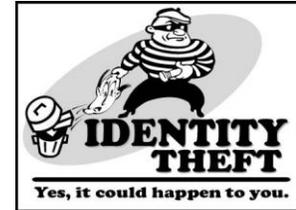


Guard Your Numbers

Identity thieves can hit the jackpot with your Social Security number or financial account numbers, but they also value the ordinary numbers you use in your everyday life. Here are a few they try to obtain and some ways to protect yourself.



- **Birth date** – With your name, address and birth date in hand, crooks may be able to buy your Social Security number on websites that normally sell them to businesses conducting background checks. If they cannot, just by knowing your birth date and city, scammers can often guess most, if not all, the digits of your Social Security number. Some businesses do need your birth date to verify your identity, such as health care providers and credit card companies, but most others do not. Think twice before providing it to merchants who might be vulnerable to a data breach by hackers. Forgo birthday freebies businesses offer and never post your birth date on social media sites or on any other public websites.
- **ZIP code** – You may be asked for it when you pay with a credit card at a store’s cash register. Beware – the purpose may be to figure out your address so you can be put on a mailing list and bombarded with junk mail or nuisance calls. Or worse, your ZIP code may find its way to scammers who will couple it with other bits of personal data to steal your identity. Generally you have to provide a ZIP code when you use a credit card at an untended machine, such as a gasoline pump, which is an added security measure to foil thieves, but it is usually unnecessary at stores. Your ZIP code should not be posted on social media or other public websites.
- **Phone number** – Your phone number may be unlisted or blocked for caller ID, but special online software can allow phone fraudsters to still see it. When you receive robocalls, responding to “opt out” instructions may merely serve to notify the caller that your number is working and ripe for future calls. Just hang up without pressing any key. Making callbacks to offers of free merchandise also reveals your phone number, which can then end up on “sucker lists” that scammers sell to each other online through information black markets.
- **Passport** – Even if you are not traveling, a lost or stolen passport is serious business. Its number can open the door to identity theft. So at home and abroad, keep your passport securely locked away. If it goes missing in the U.S., call the State Department toll-free at 877-487-2778 to immediately deactivate it and get a new one. If you are abroad, contact the nearest U.S. embassy or consulate. You can get the address and phone number online at www.usembassy.gov.
- **PINS** – Never use your birth date, your birth year or your home’s street address as a PIN for an ATM. That way, if your wallet falls into the hands of a thief, a quick look at your driver’s license will not translate into an unauthorized cash withdrawal. Avoid portions of your current phone number or Social Security number. Do not use those PINS on your cell phone either. Also stay away from 1234, 0000, 2580 (a top to bottom keypad sequence), 1111, 5555, 0852 (a bottom to top sequence), 2222, 1212 and 1998, as these PINs are most easily figured out by scammers.