WV Executive Branch Privacy Tip

THINKING OF PROVIDING YOUR SOCIAL SECURITY NUMBER? THINK AGAIN.

From doctor's offices and financial institutions to college university admittance applications and summer camp registrations, the request for your Social Security number (SSN) has become commonplace. In fact, it's become such a standard request that many individuals willingly provide this number without hesitation and without really thinking about the **consequences behind this**, one of which being an increased risk of identity theft.

Social Security numbers hold one of the keys to your identity. With it, you can open a new line of credit, gain employment, receive health insurance and file taxes. Thieves also know the power behind this nine-digit number, which is why it's one of the most highly sought after pieces of personal information. There are a variety of ways that thieves attempt to obtain SSNs, and they include more low-tech methods like sifting through your trash, stealing a wallet, purse or laptop; or using more sophisticated ways like phishing emails and texts, scam calls and via data breaches. For example, there were nearly **158 million social security numbers** exposed in 2017 due to data breaches.

While the exposure of your SSN is not entirely preventable – data breaches are a perfect example of this – consumers should refrain from giving it out unnecessarily to minimize their risks of identity theft. Basically, the frequency at which the number is exposed – whether intentional or unintentional, the higher the probability that it will be compromised. Here are some tips to help you protect your SSN and become a better steward of your identity:

Be in the Know – Educate yourself on the types of scenarios that require you to provide your Social Security number so that you can decide ahead of time whether or not you should provide it. Here is a list of **situations** that require your SSN:

- Internal Revenue Service for tax returns and federal loans
- Employers for wage and tax reporting purposes
- Financial institutions for monetary and credit transactions
- Veterans Administration as a hospital admission number
- Department of Labor for workers' compensation
- Department of Education for student loans
- Entities that administer any tax, general public assistance, motor vehicle or driver's license law
- Child support enforcement
- Food Stamps
- Medicaid
- Unemployment Compensation

Don't be afraid to ask – When your Social Security number is requested it's best to ask the requestor some additional information to better understand whether you absolutely need to provide your SSN and if so, how they plan to protect it. In some instances, you may be able to provide an alternative like a driver's license. Keep in mind that if you don't provide your SSN, some entities may refuse to provide the services requested. Some questions to consider asking **are**:

- Why does the company need this information (what law or reason make this a requirement)?
- How do you protect this information?
- What will happen if I don't provide it?
- Is there is an alternative to providing my SSN (driver's license, etc.)?

Protect your physical card, too – It's crucial to not only correctly safeguard your social security number but to also protect the physical card to the best of your ability. This includes storing it in a secure place (like a locked safe) and by not carrying it around in your wallet or purse.

Be leery of scammers – Scammers may **pose as the IRS**, the Social Security Administration and others to attempt to gain access to your SSN and they may do so over the phone, through email, text or even through social media platforms. To stay safe, never provide your SSN or other sensitive information on a call that you didn't initiate. Also, don't automatically give out your Social Security number via email, text or social media messages, even if it looks like a legitimate business requesting it. Instead, call the entity directly by locating their number on their official website, on the back of your card or even on a recent bill.
If you know your social security number has been compromised, contact our advisors using our toll-free number (888-400-5530) and they can inform you about the necessary steps to take to resolve the issue. You can also reach us using our live chat feature.

---

*Contact the Identity Theft Resource Center for toll-free, no-cost assistance at (888) 400-5530. For on-the-go assistance, check out the **free ID Theft Help App** from ITRC.*