Grave Mistakes: Thousands of Names, SSN's, Dates of Birth, Released in Error

By Denise Richardson

October 28, 2011 - We all know that identity thieves can strike from anywhere, and leaks of sensitive data that can potentially expose individuals to identity theft happen frequently. Sometimes these leaks come from places that you wouldn't expect, and often go on for months or even years before they're discovered. One such leak has been going on since 1980, and still continues today.

Tweet

```
(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();
```

```
 (function() {
   var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
   po.src = 'https://apis.google.com/js/plusone.js';
   var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
 })();
```

If you think that sounds bad, it gets worse; the leak, which is estimated to release approximately 14,000 Social Security numbers per year, comes from the Social Security Administration itself.

That's right, according to an investigative report "Grave Mistakes" by the Scripps Howard News Service, since 1980 the SSA has released an estimated 400,000 active Social Security numbers to the public and will most likely continue releasing active Social Security numbers in the future.

The source of the leak is a public record known as the Social Security Administration's Death Master File. This record, released annually, contains the Social Security numbers of every American reported as "deceased" in the preceding year. To date the Death Master File records contain approximately 90 million entries, all of whom are supposedly deceased--but unfortunately, that's not always the case. And unfortunately -that's part of the problem. Many of these SSN's, names and dates of birth that were released--belong to people still very much alive.

Human error can strike the best of us, and when dealing with such a large volume of information it's all but inevitable. And that's part of a problem that is often overlooked when it comes to data security. Mistakes made while entering information can result in the information of people who are still alive being included in the Death Master File, which is freely available to the public at large. The 14,000 figure I mentioned earlier isn't an arbitrary figure; that's an estimate that the SSA once gave as to how many mistakes of this type are made each year when updating the Death Master File.
If you think this sounds bad, it gets worse.

Even though the Social Security Administration acknowledges that these mistakes are made, they don't inform those who have been incorrectly listed as deceased about the mix-up.

Some never find out; others find out when their bank freezes their accounts or when they have problems with their insurance, mortgage or other loans. Some even find out when applying for jobs, making it appear that they're trying to use the identity of a deceased individual to find employment.

The SSA says that they take swift action to correct any problems like this that they discover, but how long does the data remain in a public file before it gets discovered? How many problems do people have with their banks or other agencies before the mistake is corrected? How much trouble do these people have to go through to get these problems corrected once they occur, since they have to convince a bank, insurance company or potential employer that the Social Security Administration made a mistake?

The Social Security Administration, claims that to date there's "no evidence" that anyone has had their identity stolen as a result of these "mistakes". This is a common claim we often hear by those minimizing the potential risks after a breach of data occurs. Sadly, data breaches continue to occur at an alarming rate and down playing the seriousness of a breach sidesteps the very real problems that consumers may face for years to come.

Once our SSN is released--it's non-retrievable. That all important Social Security number can be sold multiple times to multiple thieves who have multiple uses for our personal info; accessing bank accounts, hijacking tax returns, obtaining housing, medical services, employment, utilities and government benefits such as Unemployment insurance, Medicare, and Medicaid.

The truth is, whether or not there is "evidence" indicating stolen or lost data has been used to commit fraud, doesn't mean it hasn't -and it certainly doesn't mean it never will.

As the digitization of personal data moves forward, the need for public education and personal identity monitoring grows stronger than ever. Not convinced yet? See: Can we secure digital health records?

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.