

ID Thieves Targeting Other Crooks? The Ironic Data Breach in Washington State

May 10, 2013 - Just imagine yourself in this position. You are trying to establish a false identity. You find a black market supplier who sells you a Social Security Number and other identifying information. You think you're home free. Then you find out that the information you purchased was actually from someone convicted of a crime. Well, that's just one possible scenario facing anyone who purchases data stolen from the Washington State court system.

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);
})();
```

The state court computers for Washington have been hacked. The incident started sometime after September of last year and was discovered in February of this year. And the hackers managed to gain access to a computer that stored 160,000 Social Security numbers and more than 1 million driver's licenses. So far, 94 people have been told that their individual information was compromised in the hacking incident.

State officials currently believe that the 94 people notified were the only ones that had their data stolen. But they really aren't sure. Their information was apparently in a separate file from the one containing the 160,000 SSNs. But the larger file was there for the taking and doesn't appear to have been encrypted.

If the other file was stolen, whoever uses the SSNs it contained may be in for a big surprise. That file contains identifying information for people booked into a city or county jail between September 2011 and December 2012. Oops!

A third file contained information from over 1 million driver's licenses. Anyone using that information could find themselves facing another issue. A large number of those licenses belonged to people who had been arrested for a DUI between 1989 and 2011 or who resolved a criminal matter in 2011 or 2012. But it also contained information on people who resolved minor traffic infractions in 2011 and 2012.

The breach was apparently preventable. The state needed to install a software security patch on its computer system, but they had failed to do so. The state also admits that files with personally identifiable information in them should not have been stored the way that they were. They have changed their procedures for storing data and updated their software since the breach.

Anyone falling into any of the described groups above should check their credit report for errors and may want to have a fraud alert placed on their file. The State of Washington has setup a website with more information about the breach which can be found at <http://www.courts.wa.gov/databreach>. They have also setup a telephone hotline which can be

reached at 1-800-448-5584.

byJim Malmberg

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.

Follow me on Twitter:

Follow ACCESS