

LexisNexis Working with States to Prevent Taxpayer ID Theft

April 17, 2013 - Taxpayer ID theft is a growing problem for both the IRS and the individual states, and it can happen to anyone. Victims don't usually discover the crime until they file their tax returns. That's when they are notified that someone else filed a tax return in their name, using their SSN, and that whoever it was impersonating them has already been sent their tax refund. Getting the problem corrected can take months. But now LexisNexis - a company that assembles large consumer databases - is working with several states to put a halt to the problem. And initial reports appear to be promising.

[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);  
})();
```

Last year, LexisNexis introduced a new service called Tax Refund Investigative Solution (TRIS). They only made the service available to the State of Georgia initially. In the first year that the service was in place, it appears to have enabled the state to stop more than \$23 million in fraudulent refunds.

This year, the company is working with four states; Connecticut, Georgia, Louisiana and South Carolina. And the company has announced that it is in talks with other states as well.

One of the primary reasons that tax ID theft has become a popular crime is that there are few barriers to entry for criminals. If a crook can get their hands on your SSN, they simply file a fraudulent tax return electronically. No need to walk into an IRS office. No need to interact with anyone on a face to face basis. Simply fill in the information, give a return address for the refund to be sent to, and click to submit. Now all the thief has to do is wait for the tax return to show up in the mail; usually at a PO Box that can't be traced back to the crook.

Enter LexisNexis. Commercial consumer databases often contain significantly more information about you than any government agency has access to. Overall, we'd have to say that commercial databases are not consumer friendly. If nothing else, they present themselves as attractive targets for ID thieves themselves. They also present other privacy concerns.

So we find it to be no small irony that in this case, a large commercial database is actually being used to prevent crime.

The TRIS concept appears to be fairly simple. When someone submits a tax return in one of the participating states, the information they supply is compared to the information contained in LexisNexis own database. So if someone files a tax return and uses an address that has never been associated with their name and SSN, a red flag is raised. When that

happens, the person filing the return is asked a series of questions that only they should be able to answer. If they can't answer the questions, the return isn't processed.

Red flags may not be associated with just addresses. Any other suspicious information contained in a filing could trigger the challenge questions.

Of course, the need for such a product would be significantly reduced if the states and the IRS would allow everyone to select a password for authentication.

by Jim 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