From: Tom Young <tyoung@tomyounglaw.com>
To: Pitts, TedTedPitts@gov.sc.gov
CC: Veldran, KatherineKatherineVeldran@gov.sc.gov
Stirling, BryanBryanStirling@gov.sc.gov
Date: 10/31/2012 5:08:21 PM
Subject: RE: Legislative follow up

Ted:

More questions:

1. When can dependents be enrolled? If not now, why not?

2. According to the recording at this number, you are only eligible to receive the free year of credit monitoring if you are currently a South Carolina resident. This does not protect anyone who works in SC and lives elsewhere, nor does it protect former residents of SC that have since moved away. Why is that? Is something being done about this?

3. Were 3.6 Million ssn's involved or 3.6 Million tax returns?

4. How does someone know if their SSN has been affected? Ie one of the ones taken in the attack?

5. Did the hacker(s) get the bank account and routing info for SC taxpayers who pay taxes by bank draft?

6. Are business tax id numbers affected?

7. Are business bank account numbers affected? Could they have been taken by the hacker?

8. Are business credit card numbers affected?

9. How to respond to these from constituents?

    a. I don't think I'll ever understand the reasoning behind distributing the same activation code to millions of people. This, in my mind, defeats the purpose of an activation code. But nevertheless, the activation code, because it is the same for everyone, and because there to be no real way for a citizen to determine if their information was affected, is being used unnecessarily by individuals who may not be affected. This is a complete and utter waste of money. I have not seen reported yet how much money is being spent to provide "affected" South Carolinians with this year of credit monitoring, but however much it is, it should be minimized as much as possible.

    b. Citizens are being led to believe as long as they sign up for this year of credit monitoring, they'll be ok. This is simply not true. If the credit monitoring service determines that your information is being used without your consent, you are the one still responsible for resolving the issue, and potentially still liable for the damage if it can't be proven to be linked to this incident. And what's one year? Big whoop, a smart criminal will simply sit on the information and use it after a year so that it is less likely to be tracked to one particular data breech. Sure, ProtectMyID will be happy to allow "consumers to continue to have access to fraud resolution agents and services beyond the first year," for a fee. This free year of credit monitoring is merely a band-aid on a gushing wound and ultimately not very effective at minimizing the damage that's been done. Attached is a brochure that was shared with me from a representative at SRP Federal Credit Union describing a much more effective approach to protecting your identity. Citizens will be far better protected if they place a security freeze on their credit reports as described in this brochure. Citizens also need to be informed that since their dependents' Social Security Numbers are included on tax returns, it's highly likely their information was stolen as well. Not many

people monitor the credit reports of their minor dependents, but this is also a necessary step to minimize damage.

c. Can the governor really just spend extremely excessive amounts of state money without any approval from Congress?

d. How is it possible that a state agency such as the DOR is not required to encrypt our information? It is absolutely outrageous and incompetent for only a portion of the payment card information and none of the Social Security numbers to have been encrypted.

e. What assessment is being conducted to ensure the strategies put in place to manage this fiasco are actually effective? The governor wants complete transparency from higher education and other agencies, and assessment matrices in place to ensure adequate measuring of performance, but I have seen no attempt to measure the extent of damage being done with our stolen information.

Thank you.

Tom

From: Pitts, Ted [mailto:TedPitts@gov.sc.gov]
Sent: Tuesday, October 30, 2012 7:11 PM
To: Pitts, Ted
Cc: Veldran, Katherine; Stirling, Bryan
Subject: Legislative follow up

All,

I am having the attorneys, Experian, SLED, the Inspector General and SCDOR review the answers to the questions we have received. We want to make sure that you have accurate information to distributed to your constituents.

Below are answers to the most frequently asked questions that I can confirm:

Are young adults that previously filed in SC covered? If a tax return was filed from 1998 until present and a person's SS# was listed on the return as the filer or a dependent they can sign up for the protection. Individuals currently 18 and older must enroll themselves. Individuals currently 17 and younger must be added on the family plan by their parent or legal guardian. Laws do not allow them to consent to this agreement on their own. SCDOR will cross check SS#s with all enrollments.

Why doesn't SCDOR just enroll taxpayers? It is against the law to enroll taxpayers without their consent.

Could we not have a portal provided that would allow quicker, more direct and easier access? Experian has a South Carolina portal/page it is- www.protectmyid.com/scdor . The activation code is SCDOR123 (not case sensitive) to enroll. A way to confirm that you are on the correct page is the picture of the person/model on the page should be a female. Some people are being bounced directly to the Experian home page (the picture on this page is a male) this is a problem on the user's end not Experian's. If they don't have access to the internet, they can call 1-866-578-5422. Experian is working to address wait times.

How much time should deployed, overseas military expect to wait before they are contacted? Is there any "extra" contact, perhaps specifically assigned to this group, that we can share to get them in touch with the right people without having a phone line wait? We are in the process of working with the Department of Defense to make the notification enrollment process as easy as possible. Details will be released when confirmed.

Were checking account routing numbers compromised? Of the files accessed an individual's entire return was

accessed. The Social Security #'s and bank information were not encrypted. Credit cards were encrypted on returns older 2003. Any unencrypted credit card information would be for cards that have expired.

We will follow up as soon as possible regarding other questions, our goal is to email the General Assembly a comprehensive FAQs packet as soon as it is finished.

Thanks,
Ted

Ted Pitts
Deputy Chief of Staff
Governor Nikki Haley
Cabinet and Legislative Affairs
803.767.7862
TedPitts@gov.sc.gov