Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Thursday, November 01, 2012 6:13 PM
To: Godfrey, Rob
Subject: question on hole being closed on 10/20

From Budget and Control Board:

The Cyber Security Network Monitoring services monitor network traffic and identify unusual network activity. Network sensors are installed within the network of an agency that will alert DSIT of any unusual activity. Once DSIT alerts an agency of unusual network activity, the agency is responsible for addressing and determining the full extent of the incident.

No, DSIT does not charge agencies for these services.

Full network monitoring was instituted for the Department of Revenue on 10/20/12. At the Department of Revenue's request, DSIT did monitor certain workstation activity at their Gervais Street location. DSIT was not asked to monitor the systems where the breached data was housed.

Question:
With the fact that the systems where the breached data was housed are monitored as of 10/20, is this what the governor is referencing when she talks about the hole being closed on 10/20?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Thursday, November 01, 2012 6:40 PM
To: Samantha Cheek
Cc: Godfrey, Rob
Subject: RE: additional assistance for elderly

Importance: High

Why did DOR use the monitoring for some computers but not the ones that were breached? Where are the breached computers housed? Whose decision was it to decline the protection for the breached computers?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

From: Samantha Cheek [CheekS@sctax.org]
Sent: Thursday, November 01, 2012 6:20 PM
To: Largen, Stephen
Subject: Re: additional assistance for elderly

Those details are available in the Chronology available on the cyber attack portion of our website. The "hole" that she is referring to is the one that Mandiant was hired to monitor within DOR's servers.

Samantha Cheek
SC Department of Revenue
(803) 898-5281

On Nov 1, 2012, at 6:03 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:

> Budget and Control Board says full network monitoring was instituted on Oct. 20. Is that the hole the governor has repeatedly referenced as being closed on that date?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 5:52 PM
> To: Largen, Stephen
> Subject: RE: additional assistance for elderly
>
> At this point the only details that I can give to you is that DOR
> servers are being monitored by DSIT as of October 11.
>
> -----Original Message-----
> From: Largen, Stephen [mailto:slargen@postandcourier.com]

> Sent: Thursday, November 01, 2012 5:31 PM
> To: Samantha Cheek
> Subject: RE: additional assistance for elderly
>
> Samantha,
> Which DOR offices were using Division of State IT cyber protection at
> the time the breach was discovered on Oct. 10? My understanding is
> that the system that was breached did not have this protection in
> place. Why was that? Has that changed since the breach?
>
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
>

Godfrey, Rob

From: Shain, Andy <ashain@thestate.com>
Sent: Thursday, November 01, 2012 6:53 PM
To: Godfrey, Rob
Subject: Re: Follow up

OK

On Thu, Nov 1, 2012 at 6:52 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

Quote from Rob Godfrey, Haley spokesman: "The governor has asked the Inspector General to report to her about how to strengthen IT security, and she looks forward to receiving his report and then moving forward to make South Carolina state government's IT security as strong as possible."

Rob Godfrey
Office of Gov. Nikki Haley

O: (803) 734-5074 | C: (803) 429-5086

--
Andrew Shain
Reporter/Editor
The State
1401 Shop Road
Columbia, S.C. 29201
(803) 771-8619
Web: thestate.com
Twitter: @andyshain

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Thursday, November 01, 2012 6:53 PM
To: Largen, Stephen
Cc: Godfrey, Rob
Subject: Re: additional assistance for elderly

DOR uses the same protection for all computers throughout the agency. Protection was not declined for the computers. We cannot comment on where the breached computers were housed.

Samantha Cheek
SC Department of Revenue
(803) 898-5281

On Nov 1, 2012, at 6:41 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:

> Why did DOR use the monitoring for some computers but not the ones that were breached? Where are the breached computers housed? Whose decision was it to decline the protection for the breached computers?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 6:20 PM
> To: Largen, Stephen
> Subject: Re: additional assistance for elderly
>
> Those details are available in the Chronology available on the cyber attack portion of our website. The "hole" that she is referring to is the one that Mandiant was hired to monitor within DOR's servers.
>
> Samantha Cheek
> SC Department of Revenue
> (803) 898-5281
>
> On Nov 1, 2012, at 6:03 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>
>> Budget and Control Board says full network monitoring was instituted on Oct. 20. Is that the hole the governor has repeatedly referenced as being closed on that date?
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>> Sent: Thursday, November 01, 2012 5:52 PM
>> To: Largen, Stephen

>> Subject: RE: additional assistance for elderly
>>
>> At this point the only details that I can give to you is that DOR
>> servers are being monitored by DSIT as of October 11.
>>
>> -----Original Message-----
>> From: Largen, Stephen [mailto:slargen@postandcourier.com]
>> Sent: Thursday, November 01, 2012 5:31 PM
>> To: Samantha Cheek
>> Subject: RE: additional assistance for elderly
>>
>> Samantha,
>> Which DOR offices were using Division of State IT cyber protection at
>> the time the breach was discovered on Oct. 10? My understanding is
>> that the system that was breached did not have this protection in
>> place. Why was that? Has that changed since the breach?
>>
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>>

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Thursday, November 01, 2012 6:58 PM
To: Godfrey, Rob
Subject: questions

Does the governor stand by her statements that nothing could have been done to prevent the breach in light of the fact the DOR elected not to use state protection for the breached computers?

Sen. Sheheen said: "It means I think we have to call into question what the department of revenue isn't telling us. I think we really have to look for some objective investigation into what actually occurred."
Care to respond?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

Godfrey, Rob

From: Harry Cooper <COOPERH@sctax.org>
Sent: Thursday, November 01, 2012 6:57 PM
To: Godfrey, Rob
Subject: Re: additional assistance for elderly

Samantha is drafting response now.

Sent from my iPhone

On Nov 1, 2012, at 6:47 PM, "Godfrey, Rob" <RobGodfrey@gov.sc.gov> wrote:

>
>
> -----Original Message-----
> From: Largen, Stephen [mailto:slargen@postandcourier.com]
> Sent: Thursday, November 01, 2012 6:40 PM
> To: Samantha Cheek
> Cc: Godfrey, Rob
> Subject: RE: additional assistance for elderly
> Importance: High
>
> Why did DOR use the monitoring for some computers but not the ones that were breached? Where are the breached computers housed? Whose decision was it to decline the protection for the breached computers?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 6:20 PM
> To: Largen, Stephen
> Subject: Re: additional assistance for elderly
>
> Those details are available in the Chronology available on the cyber attack portion of our website. The "hole" that she is referring to is the one that Mandiant was hired to monitor within DOR's servers.
>
> Samantha Cheek
> SC Department of Revenue
> (803) 898-5281
>
> On Nov 1, 2012, at 6:03 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>
>> Budget and Control Board says full network monitoring was instituted on Oct. 20. Is that the hole the governor has repeatedly referenced as being closed on that date?
>>
>> Stephen Largen
>> Reporter, The Post and Courier

>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>> Sent: Thursday, November 01, 2012 5:52 PM
>> To: Largen, Stephen
>> Subject: RE: additional assistance for elderly
>>
>> At this point the only details that I can give to you is that DOR
>> servers are being monitored by DSIT as of October 11.
>>
>> -----Original Message-----
>> From: Largen, Stephen [mailto:slargen@postandcourier.com]
>> Sent: Thursday, November 01, 2012 5:31 PM
>> To: Samantha Cheek
>> Subject: RE: additional assistance for elderly
>>
>> Samantha,
>> Which DOR offices were using Division of State IT cyber protection at
>> the time the breach was discovered on Oct. 10? My understanding is
>> that the system that was breached did not have this protection in
>> place. Why was that? Has that changed since the breach?
>>
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>>

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Thursday, November 01, 2012 7:19 PM
To: Godfrey, Rob
Subject: FW: additional assistance for elderly

OK to use the below? Just got it.

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

From: Samantha Cheek [CheekS@sctax.org]
Sent: Thursday, November 01, 2012 7:10 PM
To: Largen, Stephen
Subject: Re: additional assistance for elderly

Before the breach, DOR was contracting Trustwave to conduct periodic reviews and the IRS was conducting audits as well of all computer systems and servers. As an agency we did not feel it was necessary to implement DSIT's monitoring. DSIT then began monitoring all servers after DOR was notified of the breach.

Samantha Cheek
SC Department of Revenue
(803) 898-5281

On Nov 1, 2012, at 6:56 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:

> I am not asking about now; we've already established entire system is protected now. I'll ask again: why were the breached computers not protected with the service at the time of the breach? Whose decision was that?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 6:52 PM
> To: Largen, Stephen
> Cc: robgodfrey@gov.sc.gov
> Subject: Re: additional assistance for elderly
>
> DOR uses the same protection for all computers throughout the agency. Protection was not declined for the computers. We cannot comment on where the breached computers were housed.
>
> Samantha Cheek
> SC Department of Revenue
> (803) 898-5281
>

> On Nov 1, 2012, at 6:41 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>
>> Why did DOR use the monitoring for some computers but not the ones that were breached? Where are the breached computers housed? Whose decision was it to decline the protection for the breached computers?
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>> Sent: Thursday, November 01, 2012 6:20 PM
>> To: Largen, Stephen
>> Subject: Re: additional assistance for elderly
>>
>> Those details are available in the Chronology available on the cyber attack portion of our website. The "hole" that she is referring to is the one that Mandiant was hired to monitor within DOR's servers.
>>
>> Samantha Cheek
>> SC Department of Revenue
>> (803) 898-5281
>>
>> On Nov 1, 2012, at 6:03 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>>
>>> Budget and Control Board says full network monitoring was instituted on Oct. 20. Is that the hole the governor has repeatedly referenced as being closed on that date?
>>>
>>> Stephen Largen
>>> Reporter, The Post and Courier
>>> (864) 641-8172
>>> follow me on Twitter @stephenlargen
>>> _____
>>> From: Samantha Cheek [CheekS@sctax.org]
>>> Sent: Thursday, November 01, 2012 5:52 PM
>>> To: Largen, Stephen
>>> Subject: RE: additional assistance for elderly
>>>
>>> At this point the only details that I can give to you is that DOR
>>> servers are being monitored by DSIT as of October 11.
>>>
>>> -----Original Message-----
>>> From: Largen, Stephen [mailto:slargen@postandcourier.com]
>>> Sent: Thursday, November 01, 2012 5:31 PM
>>> To: Samantha Cheek
>>> Subject: RE: additional assistance for elderly
>>>
>>> Samantha,
>>> Which DOR offices were using Division of State IT cyber protection
>>> at the time the breach was discovered on Oct. 10? My understanding
>>> is that the system that was breached did not have this protection in
>>> place. Why was that? Has that changed since the breach?
>>>

>>>
>>> Stephen Largen
>>> Reporter, The Post and Courier
>>> (864) 641-8172
>>> follow me on Twitter @stephenlargen
>>> _____
>>> From: Samantha Cheek [CheekS@sctax.org]
>>>

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Thursday, November 01, 2012 7:30 PM
To: Godfrey, Rob
Subject: DOR computers

This is additional info. that could help us all save some time: DSIT did monitor certain workstation at Gervais Street location but was not asked to monitor the systems where the breached info. was housed.

Why certain systems and not others if DSIT did not meet federal standard?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Thursday, November 01, 2012 8:26 PM
To: Samantha Cheek
Cc: Godfrey, Rob
Subject: RE: additional assistance for elderly

Samantha and Rob: last question for tonight--

I believe Director Etter or Chief Keel said yesterday that the hacker went into the system twice before extracting the information from the database. Can you confirm this?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

From: Samantha Cheek [CheekS@sctax.org]
Sent: Thursday, November 01, 2012 8:19 PM
To: Largen, Stephen
Subject: RE: additional assistance for elderly

Our reports show that DSIT initiated monitoring on October 11.

DSIT was not asked to monitor the breached systems as they were already being monitored by Trustwave, and Mandiant was brought in to audit these systems specifically for this incident.

-----Original Message-----
From: Largen, Stephen [mailto:slargen@postandcourier.com]
Sent: Thu 11/1/2012 7:52 PM
To: Samantha Cheek
Subject: RE: additional assistance for elderly

See the bottom of the last page. Also, which is it for full DSIT monitoring, Oct. 11 or Oct. 20?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

From: Samantha Cheek [CheekS@sctax.org]
Sent: Thursday, November 01, 2012 7:45 PM
To: Largen, Stephen
Subject: Re: additional assistance for elderly

Where have you seen that DSIT was asked to monitor computers only at the Gervais Street location?

Samantha Cheek
SC Department of Revenue
(803) 898-5281

On Nov 1, 2012, at 7:41 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:

> Why was DSIT asked to monitor some work stations at DOR's Gervais Street location but not the systems that were breached?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 7:32 PM
> To: Largen, Stephen
> Subject: RE: additional assistance for elderly
>
> It should be noted that DOR was receiving protection on a national level through Trustwave. Trustwave was listed on a national vendor list supplied by major credit card companies as being suffiently approved for protecting systems that process credit cards.
>
> -----Original Message-----
> From: Largen, Stephen [mailto:slargen@postandcourier.com]
> Sent: Thu 11/1/2012 6:54 PM
> To: Samantha Cheek
> Subject: RE: additional assistance for elderly
>
> I am not asking about now; we've already established entire system is protected now. I'll ask again: why were the breached computers not protected with the service at the time of the breach? Whose decision was that?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 6:52 PM
> To: Largen, Stephen
> Cc: robgodfrey@gov.sc.gov
> Subject: Re: additional assistance for elderly
>
> DOR uses the same protection for all computers throughout the agency. Protection was not declined for the computers. We cannot comment on where the breached computers were housed.
>
> Samantha Cheek
> SC Department of Revenue
> (803) 898-5281
>
> On Nov 1, 2012, at 6:41 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>

>> Why did DOR use the monitoring for some computers but not the ones that were breached? Where are the breached computers housed? Whose decision was it to decline the protection for the breached computers?
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>> Sent: Thursday, November 01, 2012 6:20 PM
>> To: Largen, Stephen
>> Subject: Re: additional assistance for elderly
>>
>> Those details are available in the Chronology available on the cyber attack portion of our website. The "hole" that she is referring to is the one that Mandiant was hired to monitor within DOR's servers.
>>
>> Samantha Cheek
>> SC Department of Revenue
>> (803) 898-5281
>>
>> On Nov 1, 2012, at 6:03 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>>
>>> Budget and Control Board says full network monitoring was instituted on Oct. 20. Is that the hole the governor has repeatedly referenced as being closed on that date?
>>>
>>> Stephen Largen
>>> Reporter, The Post and Courier
>>> (864) 641-8172
>>> follow me on Twitter @stephenlargen
>>> _____
>>> From: Samantha Cheek [CheekS@sctax.org]
>>> Sent: Thursday, November 01, 2012 5:52 PM
>>> To: Largen, Stephen
>>> Subject: RE: additional assistance for elderly
>>>
>>> At this point the only details that I can give to you is that DOR
>>> servers are being monitored by DSIT as of October 11.
>>>
>>> -----Original Message-----
>>> From: Largen, Stephen [mailto:slargen@postandcourier.com]
>>> Sent: Thursday, November 01, 2012 5:31 PM
>>> To: Samantha Cheek
>>> Subject: RE: additional assistance for elderly
>>>
>>> Samantha,
>>> Which DOR offices were using Division of State IT cyber protection
>>> at the time the breach was discovered on Oct. 10? My understanding
>>> is that the system that was breached did not have this protection in
>>> place. Why was that? Has that changed since the breach?
>>>
>>>
>>> Stephen Largen

>>> Reporter, The Post and Courier
>>> (864) 641-8172
>>> follow me on Twitter @stephenlargen
>>> _____
>>> From: Samantha Cheek [CheekS@sctax.org]
>
>

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Thursday, November 01, 2012 8:35 PM
To: Largen, Stephen
Cc: Godfrey, Rob
Subject: Re: additional assistance for elderly

That's correct.

Samantha Cheek
SC Department of Revenue
(803) 898-5281

On Nov 1, 2012, at 8:28 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:

> Samantha and Rob: last question for tonight--
>
> I believe Director Etter or Chief Keel said yesterday that the hacker went into the system twice before extracting the information from the database. Can you confirm this?
>
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen
> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 8:19 PM
> To: Largen, Stephen
> Subject: RE: additional assistance for elderly
>
> Our reports show that DSIT initiated monitoring on October 11.
>
> DSIT was not asked to monitor the breached systems as they were already being monitored by Trustwave, and Mandiant was brought in to audit these systems specifically for this incident.
>
>
> -----Original Message-----
> From: Largen, Stephen [mailto:slargen@postandcourier.com]
> Sent: Thu 11/1/2012 7:52 PM
> To: Samantha Cheek
> Subject: RE: additional assistance for elderly
>
> See the bottom of the last page. Also, which is it for full DSIT monitoring, Oct. 11 or Oct. 20?
>
> Stephen Largen
> Reporter, The Post and Courier
> (864) 641-8172
> follow me on Twitter @stephenlargen

> _____
> From: Samantha Cheek [CheekS@sctax.org]
> Sent: Thursday, November 01, 2012 7:45 PM
> To: Largen, Stephen
> Subject: Re: additional assistance for elderly
>
> Where have you seen that DSIT was asked to monitor computers only at the Gervais Street location?
>
> Samantha Cheek
> SC Department of Revenue
> (803) 898-5281
>
> On Nov 1, 2012, at 7:41 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>
>> Why was DSIT asked to monitor some work stations at DOR's Gervais Street location but not the systems that were breached?
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>> Sent: Thursday, November 01, 2012 7:32 PM
>> To: Largen, Stephen
>> Subject: RE: additional assistance for elderly
>>
>> It should be noted that DOR was receiving protection on a national level through Trustwave. Trustwave was listed on a national vendor list supplied by major credit card companies as being suffiently approved for protecting systems that process credit cards.
>>
>> -----Original Message-----
>> From: Largen, Stephen [mailto:slargen@postandcourier.com]
>> Sent: Thu 11/1/2012 6:54 PM
>> To: Samantha Cheek
>> Subject: RE: additional assistance for elderly
>>
>> I am not asking about now; we've already established entire system is protected now. I'll ask again: why were the breached computers not protected with the service at the time of the breach? Whose decision was that?
>>
>> Stephen Largen
>> Reporter, The Post and Courier
>> (864) 641-8172
>> follow me on Twitter @stephenlargen
>> _____
>> From: Samantha Cheek [CheekS@sctax.org]
>> Sent: Thursday, November 01, 2012 6:52 PM
>> To: Largen, Stephen
>> Cc: robgodfrey@gov.sc.gov
>> Subject: Re: additional assistance for elderly
>>

>> DOR uses the same protection for all computers throughout the agency. Protection was not declined for the computers. We cannot comment on where the breached computers were housed.
>>
>> Samantha Cheek
>> SC Department of Revenue
>> (803) 898-5281
>>
>> On Nov 1, 2012, at 6:41 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>>
>>> Why did DOR use the monitoring for some computers but not the ones that were breached? Where are the breached computers housed? Whose decision was it to decline the protection for the breached computers?
>>>
>>> Stephen Largen
>>> Reporter, The Post and Courier
>>> (864) 641-8172
>>> follow me on Twitter @stephenlargen
>>> _____
>>> From: Samantha Cheek [CheekS@sctax.org]
>>> Sent: Thursday, November 01, 2012 6:20 PM
>>> To: Largen, Stephen
>>> Subject: Re: additional assistance for elderly
>>>
>>> Those details are available in the Chronology available on the cyber attack portion of our website. The "hole" that she is referring to is the one that Mandiant was hired to monitor within DOR's servers.
>>>
>>> Samantha Cheek
>>> SC Department of Revenue
>>> (803) 898-5281
>>>
>>> On Nov 1, 2012, at 6:03 PM, "Largen, Stephen" <slargen@postandcourier.com> wrote:
>>>
>>>> Budget and Control Board says full network monitoring was instituted on Oct. 20. Is that the hole the governor has repeatedly referenced as being closed on that date?
>>>>
>>>> Stephen Largen
>>>> Reporter, The Post and Courier
>>>> (864) 641-8172
>>>> follow me on Twitter @stephenlargen
>>>> _____
>>>> From: Samantha Cheek [CheekS@sctax.org]
>>>> Sent: Thursday, November 01, 2012 5:52 PM
>>>> To: Largen, Stephen
>>>> Subject: RE: additional assistance for elderly
>>>>
>>>> At this point the only details that I can give to you is that DOR
>>>> servers are being monitored by DSIT as of October 11.
>>>>
>>>> -----Original Message-----
>>>> From: Largen, Stephen [mailto:slargen@postandcourier.com]
>>>> Sent: Thursday, November 01, 2012 5:31 PM
>>>> To: Samantha Cheek
>>>> Subject: RE: additional assistance for elderly

>>>>
>>>> Samantha,
>>>> Which DOR offices were using Division of State IT cyber protection
>>>> at the time the breach was discovered on Oct. 10? My understanding
>>>> is that the system that was breached did not have this protection
>>>> in place. Why was that? Has that changed since the breach?
>>>>
>>>>
>>>> Stephen Largen
>>>> Reporter, The Post and Courier
>>>> (864) 641-8172
>>>> follow me on Twitter @stephenlargen
>>>> _____
>>>> From: Samantha Cheek [CheekS@sctax.org]
>

Godfrey, Rob

From: Walter [redacted] <[redacted]@hotmail.com>
Sent: Friday, November 02, 2012 5:35 AM
To: Godfrey, Rob
Subject: A job for the Governor's spokesman

Please tell me, sir---what with this being public information---I wonder why this little piece of "dirt" is seemingly being swept under the rug? Has the Governor no comment on this information? (Link to the story regarding the account manager at SCDOR being arrested to follow)

Oh wait. I know. This is not a court of law and the defendant has not been convicted of any crime. With that being said, I suppose this little tidbit is perhaps a part of the "investigation" the Governor has said she is not "allowed" to talk about---with a wink and a nod to, Mr Keel in her video.

True, the State of South Carolina certainly has it full measure of tractable dullards that gladly suck up the propaganda you so artfully help the Governor broadcast. Then again, there may be more folks becoming enlightened than you may think.

This is after all the "Age of Information". Too bad you and your boss don't understand that while you think you may control a good deal of it, you can not stop a good ole grassroots movement to expose the two of you and your minions.

http://www.wmbfnews.com/story/19798962/lewd-act-suspects-exposed-to-undercover-officers

Oh and if you should decide to respond to me, please save the phone call offer for the dullards. No wink and a nod for me, thank you very much. Put it in writing. But then, you may believe there may be a trial lawyer with a hand out and a tissue waiting to respond. (Tissue? Really? That was absolutely laughable!)

I do suppose I owe the Governor a debt of gratitude for not handing my initial complaint with sagacious clarity. Had she acted with wisdom, and aplomb, I would probably not have found it necessary to take the actions I have taken to expose her for what she is. You do know what she is do you not? Wink wink.

Thank you for your time, and I will thank you in advance for forwarding this message to the Governor. Until then I remain,

respectfully yours,

Walter [redacted]

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Friday, November 02, 2012 10:03 AM
To: Godfrey, Rob
Subject: Mandiant

I am going to send over the questions, but explain to me why we're doing it this way (will have to explain to readers). Is the guy from Mandiant in Columbia?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

Godfrey, Rob

From: Largen, Stephen <slargen@postandcourier.com>
Sent: Friday, November 02, 2012 10:29 AM
To: Godfrey, Rob
Subject: RE: Mandiant

That email doesn't work. Maybe two Ls in Marshall?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

From: Godfrey, Rob [RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 10:06 AM
To: Largen, Stephen
Subject: RE: Mandiant

You can feel free to reach out to the guy yourself. Marshal.Heilman@mandiant.com

-----Original Message-----
From: Largen, Stephen [mailto:slargen@postandcourier.com]
Sent: Friday, November 02, 2012 10:03 AM
To: Godfrey, Rob
Subject: Mandiant

I am going to send over the questions, but explain to me why we're doing it this way (will have to explain to readers). Is the guy from Mandiant in Columbia?

Stephen Largen
Reporter, The Post and Courier
(864) 641-8172
follow me on Twitter @stephenlargen

Godfrey, Rob

From: Behre, Robert <rbehre@postandcourier.com>
Sent: Friday, November 02, 2012 10:39 AM
To: Godfrey, Rob
Subject: Story on the hacking

Rob,

I'm doing a piece on how this data breach might affect Gov. Haley's re-election chances.

I would like to talk with her, if possible, or get some sort of statement about to what extent she thinks this might be relevant to South Carolinians two years from now.

I appreciate your help on this.

Best,

Robert Behre

834-937-5771

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, November 02, 2012 10:44 AM
To: Godfrey, Rob
Subject: FW: Sign ups

-----Original Message-----
From: Smith, Tim [mailto:tcsmith@greenvillenews.com]
Sent: Friday, November 02, 2012 10:37 AM
To: Samantha Cheek
Subject: Sign ups

Samantha,

Doing a story on why more people have not signed up by now for Experian.

Are you getting any feedback that might explain this?

Tim Smith
The Greenville News/Columbia Bureau

Godfrey, Rob

From: Smith, Tim <tcsmith@greenvillenews.com>
Sent: Friday, November 02, 2012 10:55 AM
To: Godfrey, Rob
Subject: DSIT

Rob,

Can you tell me if the Inspector General knew the Department of Revenue was not using DSIT's network monitoring services agency wide when he did their evaluation?

Thanks!

Tim Smith
The Greenville News/Columbia Bureau

Godfrey, Rob

From: Marshall Heilman <Marshall.Heilman@mandiant.com>
Sent: Friday, November 02, 2012 11:08 AM
To: Godfrey, Rob
Subject: RE: For review

Importance: High

Rob,

I believe this is a true statement. You are absolutely required to use a PCI Council approved vendor to protect your PCI environment. One thing to note is that Trustwave was only required to attest to the security of your PCI environment, not necessarily your PII data (tax returns, etc.).

r/
Marshall
Director
+1 (808) 230-4707

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 11:04 AM
To: Marshall Heilman
Subject: For review

"The Department of Revenue used TrustWave, one of the world's leading information technology and data security firms, because the department, as with any entity handling credit card information, is required be PCI compliant by the world's major credit card companies to safeguard financial information. DSIT, while a wonderful program, does not provide PCI compliance, and therefore the department was required to use a third-party vendor such as TrustWave."

Rob Godfrey
Office of Gov. Nikki Haley
O: (803) 734-5074 | C: (803) 429-5086

Godfrey, Rob

From: Behre, Robert <rbehre@postandcourier.com>
Sent: Friday, November 02, 2012 11:08 AM
To: Godfrey, Rob
Subject: RE: Story on the hacking

Today. Earlier would be better, but I understand she's busy. As long as I talked with her by 6 p.m. that would be fine.

- Robert
-

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 10:49 AM
To: Behre, Robert
Subject: RE: Story on the hacking

What is your deadline?

From: Behre, Robert [mailto:rbehre@postandcourier.com]
Sent: Friday, November 02, 2012 10:39 AM
To: Godfrey, Rob
Subject: Story on the hacking

Rob,

I'm doing a piece on how this data breach might affect Gov. Haley's re-election chances.

I would like to talk with her, if possible, or get some sort of statement about to what extent she thinks this might be relevant to South Carolinians two years from now.

I appreciate your help on this.

Best,

Robert Behre

834-937-5771

Godfrey, Rob

From: Behre, Robert <rbehre@postandcourier.com>
Sent: Friday, November 02, 2012 11:33 AM
To: Godfrey, Rob
Subject: RE: Story on the hacking

Thanks

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 11:24 AM
To: Behre, Robert
Subject: RE: Story on the hacking

Quote from Rob Godfrey, Haley spokesman: "That's the furthest thing from the governor's mind. Her focus is on getting to the bottom of the international hacking case, making sure citizens are as protected as possible, and preventing it from happening again. South Carolinians are just finishing up one long election season, they are rightly not focused on another one, and neither is Governor Haley. As with job creation, government reform, and so many other vital issues, Governor Haley has always believed that the politics will take care of itself if she continues to work hard and get results for the people of our state."

From: Behre, Robert [mailto:rbehre@postandcourier.com]
Sent: Friday, November 02, 2012 11:08 AM
To: Godfrey, Rob
Subject: RE: Story on the hacking

Today. Earlier would be better, but I understand she's busy. As long as I talked with her by 6 p.m. that would be fine.

- Robert
-

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 10:49 AM
To: Behre, Robert
Subject: RE: Story on the hacking

What is your deadline?

From: Behre, Robert [mailto:rbehre@postandcourier.com]
Sent: Friday, November 02, 2012 10:39 AM
To: Godfrey, Rob
Subject: Story on the hacking

Rob,

I'm doing a piece on how this data breach might affect Gov. Haley's re-election chances.

I would like to talk with her, if possible, or get some sort of statement about to what extent she thinks this might be relevant to South Carolinians two years from now.

I appreciate your help on this.

Best,

Robert Behre

834-937-5771

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, November 02, 2012 11:44 AM
To: Godfrey, Rob
Subject: Greenville News

Rob.... Please advise or I can go with the previous statement:

Can you also give me a response to why the Department of Revenue did not utilize the network monitoring services offered by DSIT agency wide until Oct. 20?

Thanks!

Tim Smith

Samantha Cheek
Public Information Director
SC Department of Revenue
P.O. Box 125, Columbia, SC 29214
P: 803.898.5281 | F: 803.898.5020
www.sctax.org | Twitter: @SCDOR

Godfrey, Rob

From: Adcox, Seanna M. <SAdcox@ap.org>
Sent: Friday, November 02, 2012 12:01 PM
To: Godfrey, Rob
Subject: Expired credit cards

So, I do still have questions on the expired card front:

_How can officials emphatically say that any unencrypted credit card numbers were definitely expired? (Yet, we lack specific information on pretty much everything else, from whose names were taken to what kind of data.) Basically, how is everything else unknown, but this is for sure?

_And I still need an on-the-record explanation for why expired numbers are thought to be not vulnerable.

_And someone please explain the number for unencrypted credit card numbers. How do we know 16,000 were unencrypted? (Kinda goes back to the first question.) I think Etter said those were numbers in the system before 2003, but frankly I don't have that in my dictation and my recorder was too far away in the hearing to accurately pick it up. If that's the case, what's special about the year 2003? (Why did the agency start encrypting card numbers then?)

Thanks,
Seanna

msk dccc60c6d2c3a6438f0cf467d9a4938

Godfrey, Rob

From: Adcox, Seanna M. <SAdcox@ap.org>
Sent: Friday, November 02, 2012 12:09 PM
To: Godfrey, Rob
Subject: RE: Expired credit cards

5 p.m.?

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 12:02 PM
To: Adcox, Seanna M.
Subject: Re: Expired credit cards

Deadline?

From: Adcox, Seanna M. [mailto:SAdcox@ap.org]
Sent: Friday, November 02, 2012 12:00 PM
To: Godfrey, Rob
Subject: Expired credit cards

So, I do still have questions on the expired card front:

_How can officials emphatically say that any unencrypted credit card numbers were definitely expired? (Yet, we lack specific information on pretty much everything else, from whose names were taken to what kind of data.) Basically, how is everything else unknown, but this is for sure?

_And I still need an on-the-record explanation for why expired numbers are thought to be not vulnerable.

_And someone please explain the number for unencrypted credit card numbers. How do we know 16,000 were unencrypted? (Kinda goes back to the first question.) I think Etter said those were numbers in the system before 2003, but frankly I don't have that in my dictation and my recorder was too far away in the hearing to accurately pick it up. If that's the case, what's special about the year 2003? (Why did the agency start encrypting card numbers then?)

Thanks,
Seanna

msk dccc60c6d2c3a6438f0cf467d9a4938

Godfrey, Rob

From: Harry Cooper <COOPERH@sctax.org>
Sent: Friday, November 02, 2012 12:16 PM
To: Godfrey, Rob
Subject: RE: Expired credit cards

...got them.

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, November 02, 2012 12:15 PM
To: Harry Cooper; Samantha Cheek
Subject: Fw: Expired credit cards

Harry --

Per our phone call.

Rob

From: Adcox, Seanna M. [mailto:SAdcox@ap.org]
Sent: Friday, November 02, 2012 12:00 PM
To: Godfrey, Rob
Subject: Expired credit cards

So, I do still have questions on the expired card front:

_How can officials emphatically say that any unencrypted credit card numbers were definitely expired? (Yet, we lack specific information on pretty much everything else, from whose names were taken to what kind of data.) Basically, how is everything else unknown, but this is for sure?

_And I still need an on-the-record explanation for why expired numbers are thought to be not vulnerable.

_And someone please explain the number for unencrypted credit card numbers. How do we know 16,000 were unencrypted? (Kinda goes back to the first question.) I think Etter said those were numbers in the system before 2003, but frankly I don't have that in my dictation and my recorder was too far away in the hearing to accurately pick it up. If that's the case, what's special about the year 2003? (Why did the agency start encrypting card numbers then?)

Thanks,
Seanna

msk dccc60c6d2c3a6438f0cf467d9a4938

Godfrey, Rob

From: [redacted]@gmail.com on behalf of Robbie Brown <RobbieB@nytimes.com>
Sent: Friday, November 02, 2012 12:47 PM
To: Godfrey, Rob
Subject: Re: Video: Gov. Nikki Haley's Cabinet meeting and media availability

Rob,

It's Robbie from the New York Times.

Question about the security breach. Why was it not reported until Oct. 26? Doesn't the law require attacks to be reported "in the most expedient time possible and without unreasonable delay"?

Also, can you say how Mandiant was chosen? They stand to receive up to $12 million from the state. Why were they chosen over other firms?

My deadline is this afternoon. Please send me a statement as soon as possible.

Thanks,
R

On Thu, Nov 1, 2012 at 4:34 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

Video: Gov. Nikki Haley's Cabinet meeting and media availability

COLUMBIA, S.C. – Governor Nikki Haley held a Cabinet meeting today to discuss how state agencies can assist South Carolina taxpayers affected by the South Carolina Department of Revenue (DOR) information security breach.

Video of the governor's Cabinet meeting is available here:
http://www.youtube.com/watch?v=KxE8KZluW88

Video of the governor's media availability following the Cabinet meeting is available here:
http://www.youtube.com/watch?v=0MHg3NXLqnM

S.C. DOR last week announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers had been exposed in a cyber attack, and yesterday state officials said that information from up to 657,000 businesses was also exposed.

As of Thursday morning, the Experian call center set up to assist South Carolina taxpayers had received approximately 653,000 calls and approximately 521,000 signups for Experian's ProtectMyID program. Access to unlimited fraud resolution beyond the one year enrollment period is included in Experian's ProtectMyID membership and available to any taxpayer affected by DOR's information security breach. Taxpayers who sign up for protection will also be notified – by email or letter – about

how to sign up for a "Family Secure Plan" if they claim minors as dependents.

Dun & Bradstreet Credibility Corp will offer South Carolina businesses that have filed a tax return since 1998 a CreditAlert product that will alert customers to changes taking place in their business credit file starting Friday. Even something as simple as a change to a business address or a company officer change would set off an alert to the business owner. The cost will be waived for business filing tax returns since 1998. Business owners can visit http://www.dandb.com/sc/ beginning Friday or they can call customer service toll free at this dedicated phone number 1-800-279-9881.

Experian is offering those impacted South Carolina businesses Business Credit AdvantageSM - a self-monitoring service that allows unlimited access to a company's business credit report and score. Beginning Thursday, South Carolina businesses can sign up for Business Credit AdvantageSM at http://www.smartbusinessreports.com/SouthCarolina.

Gov. Haley reiterated that anyone who has filed a South Carolina tax return since 1998 should take the following steps:

- Call 1-866-578-5422 to enroll in a consumer protection service. (The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.)

- For any South Carolina taxpayer who wishes to bypass the telephone option, there currently is an online service available at http://www.protectmyid.com/scdor. Enter the code SCDOR123 when prompted. South Carolina taxpayers have until the end of January, 2013 to sign up.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year. Complimentary 12-month ProtectMyID memberships available to South Carolina taxpayers affected by the DOR information security breach include:

- **Credit Report:** A free copy of your Experian credit report.

- **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax® and TransUnion® credit reports.

- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.

Video of the governor's Cabinet meeting is available here:
http://www.youtube.com/watch?v=KxE8KZluW88

Video of the governor's media availability following the Cabinet meeting is available here:
http://www.youtube.com/watch?v=0MHg3NXLqnM

S.C. DOR last week announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers had been exposed in a cyber attack, and yesterday state officials said that information from up to 657,000 businesses was also exposed.

As of Thursday morning, the Experian call center set up to assist South Carolina taxpayers had received approximately 653,000 calls and approximately 521,000 signups for Experian's ProtectMyID program. Access to unlimited fraud resolution beyond the one year enrollment period is included in Experian's ProtectMyID membership and available to any taxpayer affected by DOR's information security breach. Taxpayers who sign up for protection will also be notified – by email or letter – about how to sign up for a "Family Secure Plan" if they claim minors as dependents.

Dun & Bradstreet Credibility Corp will offer South Carolina businesses that have filed a tax return since 1998 a CreditAlert product that will alert customers to changes taking place in their business credit file starting Friday. Even something as simple as a change to a business address or a company officer change would set off an alert to the business owner. The cost will be waived for business filing tax returns since 1998. Business owners can visit http://www.dandb.com/sc/ beginning Friday or they can call customer service toll free at this dedicated phone number 1-800-279-9881.

Experian is offering those impacted South Carolina businesses Business Credit AdvantageSM - a self-monitoring service that allows unlimited access to a company's business credit report and score. Beginning Thursday, South Carolina businesses can sign up for Business Credit AdvantageSM at http://www.smartbusinessreports.com/SouthCarolina.

Gov. Haley reiterated that anyone who has filed a South Carolina tax return since 1998 should take the following steps:

- Call 1-866-578-5422 to enroll in a consumer protection service. (The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.)

- For any South Carolina taxpayer who wishes to bypass the telephone option, there currently is an online service available at http://www.protectmyid.com/scdor. Enter the code SCDOR123 when prompted. South Carolina taxpayers have until the end of January, 2013 to sign up.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year. Complimentary 12-month ProtectMyID memberships available to South Carolina taxpayers affected by the DOR information security breach include:

- **Credit Report:** A free copy of your Experian credit report.

- **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax® and TransUnion® credit reports.

- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.

- **ExtendCARE:** Full access to the same personalized assistance from a highly-trained Fraud Resolution Agent even after your initial ProtectMyID membership expires.

- **$1 Million Identity Theft Insurance:** As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

-###-

Rob Godfrey
Office of Gov. Nikki Haley

O: (803) 734-5074 | C: (803) 429-5086

--

Robbie Brown
The New York Times
Regional News Assistant
Southern Bureau

Godfrey, Rob

From: Barr, Jody <jodybarr@wistv.com>
Sent: Friday, November 02, 2012 1:07 PM
To: Godfrey, Rob
Subject: Just checking in...

Any news about an availability today? Could the governor do anything on now knowing DOR didn't utilize every measure to protect this information?

Thanks again,

JB

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, November 02, 2012 1:57 PM
To: Godfrey, Rob
Subject: FW: News 19 WLTX FOIA Request

From: Stewart, Nathan [mailto:njstewart@WLTX.GANNETT.COM]
Sent: Friday, November 02, 2012 1:46 PM
To: Samantha Cheek
Subject: News 19 WLTX FOIA Request

Samantha,

DSIT tells us today that "Full network monitoring was instituted on 10/20/12. At the Department of Revenue's request, DSIT did monitor certain workstation activity at their Gervais Street location. DSIT was not asked to monitor the systems where the breached data was housed."

Can you find out for us why the SCDOR did not ask to have full network monitoring before that date and why they were not asked to monitor the systems where the breached data was housed?

Thanks.

Nate Stewart
Reporter
Cell: (803) 309-9480
Work: (803) 776-9508 EXT: 274
Twitter: @WLTXNATESTEWART
Facebook: Nate Stewart WLTX
Email: NJStewart@WLTX.GANNETT.COM

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, November 02, 2012 1:57 PM
To: Godfrey, Rob
Subject: FW: Some Questions Regarding Network Monitoring

From: Steve Dunning [mailto:Steve.Dunning@foxcarolina.com]
Sent: Friday, November 02, 2012 1:41 PM
To: Samantha Cheek
Subject: Some Questions Regarding Network Monitoring

Samantha,

I wanted to follow up on the voicemail I left you earlier today.

We'd like to speak to Director Etter regarding a letter we received from the Division of State Information Technology.

The letter states that the Dept of Revenue did not use network monitoring that is available to all state, county, education and other agencies and governments free of charge.

According to the letter, part of the Dept of Revenue's network was covered by this monitoring but the area that was breached by the hacker was not.

Can you explain why the Dept of Revenue did not want the network monitoring service provided by DSIT before October 20?

What prompted the Dept of Revenue to request it on October 20?

Could the network monitoring service have detected the hack earlier and possibly prevented the theft of so many taxpayers and businesses personal information, putting them at risk for identity theft?

If he's available we'd like to ask Director Etter these questions. If not, could you address them?

I've attached a copy of the letter below.

Sincerely,

Steve

Steve Dunning
Assignment Manager
WHNS Fox Carolina
steve.dunning@foxcarolina.com
www.foxcarolina.com
Office: (864) 213-2121
Cell: (864) 444-3708

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, November 02, 2012 1:57 PM
To: Godfrey, Rob
Subject: FW: Sign ups

-----Original Message-----
From: Smith, Tim [mailto:tcsmith@greenvillenews.com]
Sent: Friday, November 02, 2012 1:34 PM
To: Samantha Cheek
Subject: RE: Sign ups

Samantha,

Are you saying this was an either/or situation? Because DOR now uses DSIT. And was Trustweave doing "periodic" reviews? I want to be sure I am comparing apples to apples, if DSIT's monitoring was continuous.

Thanks!

Tim

From: Samantha Cheek [CheekS@sctax.org]
Sent: Friday, November 02, 2012 11:56 AM
To: Smith, Tim
Subject: RE: Sign ups

Tim, this is DOR's statement in regards to your question:

The Department of Revenue used TrustWave, one of the world's leading information technology and data security firms, because the department, as with any entity handling credit card information, is required to be PCI compliant by the world's major credit card companies to safeguard financial information. DSIT, while a wonderful program, does not provide PCI compliance, and therefore the department was required to use a third-party vendor such as TrustWave.

Thanks and I'll have a response for you soon on your other inquiry regarding Experian feedback.

Samantha Cheek
Public Information Director
SC Department of Revenue
P.O. Box 125, Columbia, SC 29214
P: 803.898.5281 | F: 803.898.5020
www.sctax.org | Twitter: @SCDOR

Godfrey, Rob

From: Robbie Brown [redacted]@gmail.com>
Sent: Friday, November 02, 2012 2:17 PM
To: Godfrey, Rob
Subject: Re: Video: Gov. Nikki Haley's Cabinet meeting and media availability

Thanks, Rob.

One more question: Do you have a response to the Post and Courier's story this morning that the hacked computers didn't have a free extra layer of security protection?

http://www.postandcourier.com/article/20121102/PC16/121109832/1165/sc-department-of-revenue-didn-t-use-state-cyber-security-system

R

On Fri, Nov 2, 2012 at 2:13 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

On the first question, please listen to South Carolina Law Enforcement Division Chief Mark Keel, during one of our daily press briefings this week: http://www.youtube.com/watch?v=ni9jQS3Nb80

The administration had a pre-existing, positive relationship with Experian, the best company in the business, through the South Carolina Department of Health and Human Services, which dealt with and vetted the company earlier this year. Experian was also willing and able to get services for taxpayers up on an expedited timeline.

Let me know what else I can do for you.

From: [redacted]@gmail.com [mailto:[redacted]@gmail.com] **On Behalf Of** Robbie Brown

Sent: Friday, November 02, 2012 12:47 PM
To: Godfrey, Rob
Subject: Re: Video: Gov. Nikki Haley's Cabinet meeting and media availability

Rob,

It's Robbie from the New York Times.

Question about the security breach. Why was it not reported until Oct. 26? Doesn't the law require attacks to be reported "in the most expedient time possible and without unreasonable delay"?

Also, can you say how Mandiant was chosen? They stand to receive up to $12 million from the state. Why were they chosen over other firms?

My deadline is this afternoon. Please send me a statement as soon as possible.

Thanks,

R

On Thu, Nov 1, 2012 at 4:34 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

Video: Gov. Nikki Haley's Cabinet meeting and media availability

COLUMBIA, S.C. – Governor Nikki Haley held a Cabinet meeting today to discuss how state agencies can assist South Carolina taxpayers affected by the South Carolina Department of Revenue (DOR) information security breach.

Video of the governor's Cabinet meeting is available here:
http://www.youtube.com/watch?v=KxE8KZluW88

Video of the governor's media availability following the Cabinet meeting is available here:
http://www.youtube.com/watch?v=0MHg3NXLqnM

S.C. DOR last week announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers had been exposed in a cyber attack, and yesterday state officials said that information from up to 657,000 businesses was also exposed.

As of Thursday morning, the Experian call center set up to assist South Carolina taxpayers had received approximately 653,000 calls and approximately 521,000 signups for Experian's ProtectMyID program. Access to unlimited fraud resolution beyond the one year enrollment period is included in Experian's ProtectMyID membership and available to any taxpayer affected by DOR's information security breach. Taxpayers who sign up for protection will also be notified – by email or letter – about how to sign up for a "Family Secure Plan" if they claim minors as dependents.

Dun & Bradstreet Credibility Corp will offer South Carolina businesses that have filed a tax return since 1998 a CreditAlert product that will alert customers to changes taking place in their business

credit file starting Friday. Even something as simple as a change to a business address or a company officer change would set off an alert to the business owner. The cost will be waived for business filing tax returns since 1998. Business owners can visit http://www.dandb.com/sc/ beginning Friday or they can call customer service toll free at this dedicated phone number 1-800-279-9881.

Experian is offering those impacted South Carolina businesses Business Credit AdvantageSM - a self-monitoring service that allows unlimited access to a company's business credit report and score. Beginning Thursday, South Carolina businesses can sign up for Business Credit AdvantageSM at http://www.smartbusinessreports.com/SouthCarolina.

Gov. Haley reiterated that anyone who has filed a South Carolina tax return since 1998 should take the following steps:

- Call 1-866-578-5422 to enroll in a consumer protection service. (The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.)

- For any South Carolina taxpayer who wishes to bypass the telephone option, there currently is an online service available at http://www.protectmyid.com/scdor. Enter the code SCDOR123 when prompted. South Carolina taxpayers have until the end of January, 2013 to sign up.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year. Complimentary 12-month ProtectMyID memberships available to South Carolina taxpayers affected by the DOR information security breach include:

- **Credit Report:** A free copy of your Experian credit report.

- **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax® and TransUnion® credit reports.

- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.

- **ExtendCARE:** Full access to the same personalized assistance from a highly-trained Fraud Resolution Agent even after your initial ProtectMyID membership expires.

- **$1 Million Identity Theft Insurance:** As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

-###-

Rob Godfrey
Office of Gov. Nikki Haley

O: (803) 734-5074 | **C:** (803) 429-5086

--

Robbie Brown
The New York Times
Regional News Assistant
Southern Bureau
RobbieB@NYTimes.com
Office: (404) 584-8645
Cell: (404) 401-4071

Godfrey, Rob

From: Results@TVEyes-Alerts.com
Sent: Friday, October 26, 2012 12:15 PM
To: Godfrey, Rob
Subject: New MMS Alert - Nikki Haley - WIS - COL (NBC)

Media Alert From TVEyes Media Monitoring Suite

(click thumbnail to play)

Nikki Haley on WIS - COL (NBC) - Columbia, SC
10/26/2012 12:13:14
WIS News 10 Midday (News)

... breaking news coming into the wis newsroom right now. governor nikki haley, sled chief mark keel, the secret service and several other state officials are planning to hold a news conference at 1:30. no details have been provided, but the state's inspector general will also be there. we are sending a crew - and will be live streaming the ...

Revenue (DOR) and Inspector General Patrick Maley will hold a press conference TODAY, Friday, October 26, at 1:30 PM. The press conference will be held at SLED headquarters.

WHO: Gov. Nikki Haley, SLED Chief Mark Keel, U.S. Secret Service, DOR Director Jim Etter and Inspector General Patrick Maley

WHAT: Press conference

WHEN: TODAY, Friday, October 26, 1:30 PM

WHERE: SLED headquarters, 4400 Broad River Road, Columbia S.C.

Note: Media should gather in SLED's lobby and will be escorted to SLED's media room.

-###-

Jeff Taillon
(803) 734-5129|Direct Line
(803) 767-7653|Cell

Godfrey, Rob

From: Neal, Sharranda <sneal@wltx.gannett.com>
Sent: Friday, October 26, 2012 12:17 PM
To: Taillon, Jeff
Cc: Jacoby, Marybeth; Godfrey, Rob; Cooke, Scott
Subject: FW: Gov. Nikki Haley, SLED Chief Mark Keel, others to hold press conference TODAY

Hi Jeff,
The email you sent out earlier, was forwarded to us from another news organization. No one here at News19 WLTX-TV received it.
When you get a chance, would you please add the following email addresses to your listserv?
News19@wltx.com
MJacoby@wltx.gannett.com
SACooke@wltx.gannett.com
SNeal@wltx.gannett.com
TSantaella@wltx.gannett.com

Thanks,

Sharranda Neal
Content Manager
News19 WLTX-TV
Address: 6027 Garners Ferry Road
Columbia, S.C. 29209
Phone: (803) 695-3741
Cell Phone: (803) [redacted]
Fax: (803) 776-1791

From: Taillon, Jeff [mailto:JeffTaillon@gov.sc.gov]
Sent: Friday, October 26, 2012 11:32 AM
To: Taillon, Jeff
Subject: Gov. Nikki Haley, SLED Chief Mark Keel, others to hold press conference TODAY

Gov. Nikki Haley, SLED Chief Mark Keel, others to hold press conference TODAY

COLUMBIA, S.C. – Governor Nikki Haley, South Carolina Law Enforcement Division (SLED) Chief Mark Keel, an official from the United States Secret Service, Jim Etter, Director of the South Carolina Department of

Godfrey, Rob

From: Smith, Tim <tcsmith@greenvillenews.com>
Sent: Friday, October 26, 2012 1:04 PM
To: Godfrey, Rob
Subject: Re: website, toll free number problems

On road call cell 864 [redacted]

Sent from my iPhone

On Oct 26, 2012, at 12:49 PM, "Godfrey, Rob" <RobGodfrey@gov.sc.gov> wrote:

> Just called you.
>
> ----- Original Message -----
> From: Smith, Tim [mailto:tcsmith@greenvillenews.com]
> Sent: Friday, October 26, 2012 12:40 PM
> To: Godfrey, Rob
> Subject: website, toll free number problems
>
> Rob,
>
> The website for taxpayers to visit requires a login. What do we tell readers? And the toll-free number has a wait. If you are asking millions of taxpayers to visit/call, we need to know how they can get through.
>
> Tim

Godfrey, Rob

From: Caula, Natalie <ncaula@postandcourier.com>
Sent: Friday, October 26, 2012 2:00 PM
To: Godfrey, Rob
Subject: Packet from Gov. Haley

Rob,

We were unable to be at the press conference. Governor Haley mentioned a packet she passed out to the press. Can any of the information be emailed to me?

Thanks,

Natalie Caula
Staff Reporter
Post and Courier
134 Columbus Street
Charleston, SC 29403
843-937-5594 Desk
843[redacted] Mobile
www.postandcourier.com
twitter.com/ncaula

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

###

happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Governor Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, October 26, 2012 2:15 PM
To: Godfrey, Rob
Subject: Re: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Done.

Samantha Cheek

SC Department of Revenue

(803) 898-5281

On Oct 26, 2012, at 2:03 PM, "Godfrey, Rob" <RobGodfrey@gov.sc.gov> wrote:

> Please make sure Natalie Caula ncaula@postandcourier.com is in receipt of the press kit ASAP.
>
> **From**: Samantha Cheek [mailto:CheekS@sctax.org]
> **Sent**: Friday, October 26, 2012 02:00 PM
> **To**: Samantha Cheek <CheekS@sctax.org>
> **Subject**: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
>
> **For Immediate Release: October 26, 2012**
>
> ### SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
>
> *Hacker illegally obtained credit card and Social Security numbers*
>
> [Columbia, S.C.] The S.C. Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.
>
> To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.
>
> "On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have

Godfrey, Rob

From: Cohen, Keven <kev@wvoc.com>
Sent: Friday, October 26, 2012 3:06 PM
To: Godfrey, Rob
Subject: from Keven Cohen

Rob---do you want five minutes for the Gov to call in with advice and to call people down? My phones are blowing up with people who are frustrated cause they can't get through.

Thanks,

Keven

Keven Cohen | The Afternoon Drive with Keven Cohen | Clear Channel Media + Entertainment
803.343.1054
316 Greystone Boulevard | Columbia | South Carolina | 29210

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

-###-

Rob Godfrey
Office of Gov. Nikki Haley
O: (803) 734-5074 | C: (803) 429-5086

Godfrey, Rob

From: Parris, Lou <lou.parris@shj.com>
Sent: Friday, October 26, 2012 3:13 PM
To: Godfrey, Rob
Subject: Automatic reply: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

The Stroller will be away from the office through Nov. 4.

Godfrey, Rob

From: Mary [redacted] <[redacted]@gmail.com>
Sent: Friday, October 26, 2012 3:16 PM
To: Godfrey, Rob
Subject: Activation Code

Rob,

The website info is useless unless you have an activation code and the phone lines are jammed.

How can we get a code?

Mary

Godfrey, Rob

From: Beeker, LaDonna <lbeeker@wistv.com>
Sent: Friday, October 26, 2012 3:20 PM
To: Godfrey, Rob
Subject: Call number issues

Hi Rob,

We are getting a lot of calls complaining about the 866-number not working and/or they can't get through because of "high call volume." Is there more than one phone number available? Or any suggestions for the callers who are getting this recording? Is the DOR working on anything else to get the public in touch with a person to find out if they have been compromised?

Please advise of any info we can give the viewers as they call and as we are coming up on future broadcasts. Thanks for your help.

LaDonna Beeker
Investigative producer
WIS-TV
803-309-6518
lbeeker@wistv.com

Godfrey, Rob

From: McQuary, Anne <amcquary@WLTX.GANNETT.COM>
Sent: Friday, October 26, 2012 3:22 PM
To: Godfrey, Rob; Taillon, Jeff
Cc: Neal, Sharranda; Santaella, Tony; Cooke, Scott; Jacoby, Marybeth
Subject: question from WLTX about the 1-866 #

Rob, Jeff,

We have tried to call the 1-866 number, it says high call volume, then it says that customer service dept is closed. Please call back between 6am-6pm or Saturday 8am-5pm.

Question is why is it saying that? Is it closed? Also will this number be open 24/7 and also on Saturday and Sunday?

Anne McQuary
Digital media producer
776-9508
www.wtlx.com

happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Gov. Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."
-###-

Rob Godfrey
Office of Gov. Nikki Haley
O: (803) 734-5074 | C: (803) 429-5086

Godfrey, Rob

From: Gatson, Judi <jgatson@wistv.com>
Sent: Friday, October 26, 2012 3:24 PM
To: Godfrey, Rob
Subject: Fwd: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
Attachments: Media_Release_10262012.pdf; ATT00001.htm

Rob,

Viewers can't get through to the number provided (tel:866-578-5422) and we can't either. Are they sure the number has been set up? Who is the best point of contact for us to get information about that phone line/service?

~ jg

Begin forwarded message:

> **From:** "Turner, Michael" <mturner@wistv.com>
> **To:** "All WIS Producers" <AllWISProducers@wistv.com>
> **Subject: FW: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers**
>
> From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
> Sent: Friday, October 26, 2012 3:06 PM
> Subject: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
>
> S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
> Hacker illegally obtained credit card and Social Security numbers
>
> COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.
>
> ***Press kit attached with information regarding the chronology of the investigation and consumer safety solutions is attached.***
>
> To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.
>
> "On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have

Godfrey, Rob

From: Howell, Jessica <jessica.howell@thepeoplesentinel.com>
Sent: Friday, October 26, 2012 3:30 PM
To: Godfrey, Rob
Subject: Out of Office AutoReply: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

I will be out of the office until Monday,October 29th. For immediate assistance, please contact our office at (803) 259-3501.
Classified Line Ad deadline is Noon on Friday.
Display Ad deadline is 5PM on Friday.

Godfrey, Rob

From: Lewis, Galan <galan.lewis@augustachronicle.com>
Sent: Friday, October 26, 2012 3:30 PM
To: Godfrey, Rob
Subject: Out of Office AutoReply: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

I will be out of the office on Friday, October 26, 2012, returning to the office on Monday, October 29, 2012. If you need immediate assistance, please contact John Gogick at john.gogick@augustachronicle.com.

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, October 26, 2012 3:31 PM
To: Ballard, Andrew; Godfrey, Rob
Subject: RE: press inquiry re cyber attack

Andrew,

As this is an ongoing criminal investigation we cannot comment as to the origin of this attack. We are unaware of any misuse of victims' confidential information related to this incident.

Regards,

Samantha Cheek
Public Information Director
SC Department of Revenue
P.O. Box 125, Columbia, SC 29214
P: 803.898.5281 | F: 803.898.5020
www.sctax.org | Twitter: @SCDOR

From: Ballard, Andrew [mailto:aballard@bna.com]
Sent: Friday, October 26, 2012 2:40 PM
To: Samantha Cheek; Rob Godfrey (RobGodfrey@gov.sc.gov)
Subject: press inquiry re cyber attack

Hello Samantha and Rob...am looking at a potential story for BNA's Privacy & Security Law Report on the cyber attack on the SC Dept of Revenue.

Was the attack from a foreign individual/entity or do we know its origin yet?

Also, are you aware of any cases of fraudulent charges/misuse of victims' bank accounts or any other situations involving identity theft?

Thanks for your time!

Andrew M. Ballard
Staff Correspondent
Raleigh, NC

BNA, Inc.

Direct 919.841.1240
aballard@bna.com

--

J. Derham Cole, Jr.
Member, S.C. House of Representatives
District 32
P.O. Box 1467
Spartanburg, SC 29304
www.derhamcole.com

No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Gov. Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

-###-

Rob Godfrey
Office of Gov. Nikki Haley

O: (803) 734-5074 | C: (803) 429-5086

Godfrey, Rob

From: [redacted]@gmail.com on behalf of Derham Cole <[redacted]@derhamcole.com>
Sent: Friday, October 26, 2012 3:47 PM
To: Godfrey, Rob
Subject: Re: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Rob,

FYI, that web link does not permit you to verify if your records have been affected. It only allows you to enter a redemption code if you already have one. The phone number is apparently overwhelmed by volume.

Thanks,
Derham

On Fri, Oct 26, 2012 at 3:06 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hacker illegally obtained credit card and Social Security numbers

COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

*****Press kit attached with information regarding the chronology of the investigation and consumer safety solutions is attached.*****

To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time.

citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

-###-

Rob Godfrey
Office of Gov. Nikki Haley

O: (803) 734-5074 | **C:** (803) 429-5086

To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Gov. Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the

Godfrey, Rob

From: Jonathan Allen <jonathan.allen@patch.com>
Sent: Friday, October 26, 2012 3:52 PM
To: Godfrey, Rob
Subject: Re: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Rob,

Thank you for sending this information along.

I know people will ask, so I'd like to have an explanation for them, why there was a 16-day lag between Oct. 10 when the state first got knowledge of the cyber attack and today when the state issued a statement about it? Did it just take that long to assess the full scale of the attack? Was it not possible to alert state residents sooner that the security of their identities are potentially at risk?

Also the 866 phone number seems to be swamped with recordings telling people to try calling back later, is the state taking measures to increase the staffing on that phone line since 3.6 million residents could potentially be calling it?

Thanks,

--
Jonathan Allen
Editor - West Ashley Patch
www.WestAshley.Patch.com
843-608-0092
843-283-9008
facebook.com/pages/West-Ashley-Patch
twitter.com/WestAshleyPatch

On Fri, Oct 26, 2012 at 3:06 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hacker illegally obtained credit card and Social Security numbers

COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

*****Press kit attached with information regarding the chronology of the investigation and consumer safety solutions is attached.*****

Godfrey, Rob

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Saturday, October 27, 2012 8:21 PM
To: Godfrey, Rob; '[redacted]@gmail.com'; Stirling, Bryan
Cc: Ken Chaplin; Joshua Light; Ken Bixler; Ozzie Fonseca
Subject: RE: Rob and Bryan, please review - TIME SENSITIVE

Just exchanged emails about 20 minutes ago; but she is waiting.

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

freecreditreport.com
freecreditscore.com
creditreport.com
protectmyid.com
safetyweb.com

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Saturday, October 27, 2012 5:19 PM
To: [redacted]@gmail.com'; Greg Young; Stirling, Bryan
Cc: Ken Chaplin; Joshua Light; Ken Bixler; Ozzie Fonseca
Subject: Re: Rob and Bryan, please review - TIME SENSITIVE

Question: are you in contact with the reporter to ensure that she understands that answers are coming her way tonight? We don't want the paper to run a story without Experian's answers and information - but more importantly we don't want the taxpayers of our state to be without the information.

Please let me know.

Rob

From: Tim Pearson [mailto:[redacted]@gmail.com]
Sent: Saturday, October 27, 2012 08:16 PM
To: Godfrey, Rob; 'Greg.Young@experianinteractive.com' <Greg.Young@experianinteractive.com>; Stirling, Bryan
Cc: 'Ken.Chaplin@experianinteractive.com' <Ken.Chaplin@experianinteractive.com>; 'Joshua.Light@experianconsumerdirect.com' <Joshua.Light@experianconsumerdirect.com>; 'Ken.Bixler@experianinteractive.com' <Ken.Bixler@experianinteractive.com>; 'ofonseca@experianinteractive.com' <ofonseca@experianinteractive.com>
Subject: Re: Rob and Bryan, please review - TIME SENSITIVE

Thanks, Greg. I think the answers to questions 3 and 4 are fine. I don't think the answers to questions 1 and 2 do enough to address the concerns of the reporter, and ultimately, the reader. And honestly, we don't know the answers - y'all do - so we'll have to rely on you for the information.

On question #1:

Will we be providing service to everyone in the state, or just those who we know to be compromised? Either option seems to me to be totally appropriate, but if it's the former, we should say so, if it is the latter, we should say so and also be prepared to explain how we distinguish the two.

On question #2:

What does the code that everyone is getting them enable them to do? Does it give them the ability to enter further information and then receive services? That was my understanding, and if that is true, we should say so.

Thanks -
Tim
Sent from my Verizon Wireless BlackBerry

From: "Godfrey, Rob" <RobGodfrey@gov.sc.gov>
Date: Sat, 27 Oct 2012 20:01:25 -0400
To: 'Greg.Young@experianinteractive.com'<Greg.Young@experianinteractive.com>; Stirling, Bryan<BryanStirling@gov.sc.gov>
Cc: 'Ken.Chaplin@experianinteractive.com'<Ken.Chaplin@experianinteractive.com>; 'Joshua.Light@experianconsumerdirect.com'<Joshua.Light@experianconsumerdirect.com>; 'Ken.Bixler@experianinteractive.com'<Ken.Bixler@experianinteractive.com>; 'ofonseca@experianinteractive.com'<ofonseca@experianinteractive.com>; '[redacted]@gmail.com'<[redacted]@gmail.com>
Subject: Re: Rob and Bryan, please review - TIME SENSITIVE

Looping Tim Pearson in.

From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Saturday, October 27, 2012 07:58 PM
To: Godfrey, Rob; Stirling, Bryan
Cc: Ken Chaplin <Ken.Chaplin@experianinteractive.com>; Joshua Light <Joshua.Light@experianconsumerdirect.com>; Ken Bixler <Ken.Bixler@experianinteractive.com>; Ozzie Fonseca <ofonseca@experianinteractive.com>
Subject: Rob and Bryan, please review - TIME SENSITIVE

Rob and Bryan,

I am not prepared to answer all of the Post and Courier questions at this point, but here are answers for the ones I feel we can answer. Obviously the paper needs this soon for EOD publishing.

1. Will you be providing your service to everyone in the state who calls and requests it, or just to those who call and you have further reason to believe their identity has been compromised? I'm not sure whether everyone can get it, or whether it just would be for certain people who may be at a higher risk (and whether you have a way of knowing that)? Some woman e-mailed me and said she tried to sign up and was being told she'd have to pay for it. **THE STATE HAS INDICATED THAT SOUTH CAROLINA TAXPAYERS DATING BACK TO 1998 SHOULD REGISTER.**
2. Right now, everyone has to call to get the same code to register for the service online (or you can wait to talk to a customer representative). I'm told on Monday, you'll have unique identifiers for everyone who calls, right? Does that mean you'll have to wait to talk to someone, or will you be able to input your

social security number (or some other sort of identifier) to get a code to go online?**THE CURRENT CODE OPOTION IS IN PLACE TO HELP WITH THE TREMENDOUS CALL VOLUME AND PROVIDE A BETTER EXPERIENCE FOR CALLERS. THE INTENT IS TO RETURN TO LIVE SUPPORT FOR ALL CALLERS ONCE THE CALL VOLUME DECREASES.**

3. Some readers e-mailed us and said they tried to register with the code, but the Web site was apparently down. How long has your Web site been unable to process SC residents' requests for protection since this was announced on Friday? **WE ARE NOT AWARE THAT THE WEB SITE HAS NEVER BEEN DOWN AND HAS HAD NO ISSUES ACCEPTING THE CODES, TO THIS POINT.**
4. What else is there we'd like to say? **AT THIS TIME, WE ARE STILL EXPERIENCING ELEVATED CALL VOLUMES, BUT THE CODE OPTION HAS BEEN WELL RECEIVED. WE ENCOURAGE INDIVIDUALS TO USE THE CODE, UNLESS THEY HAVE NO INTERNET ACCESS OR SOME OTHER REASON PREVENTS THEM FROM USING THE CODE. IN THAT CASE, THEY SHOULD CALL IN AND TALK TO A LIVE REPRESENTATIVE.**

Greg Young
Director, Public Relations
Experian Consumer Services

Godfrey, Rob

From: Stirling, Bryan
Sent: Saturday, October 27, 2012 8:26 PM
To: 'Greg.Young@experianinteractive.com'; Godfrey, Rob
Cc: 'Ken.Chaplin@experianinteractive.com'; 'Joshua.Light@experianconsumerdirect.com'; 'Ken.Bixler@experianinteractive.com'; 'ofonseca@experianinteractive.com'
Subject: Re: Rob and Bryan, please review - TIME SENSITIVE

1). All SC taxpayers from 1998 to present will be covered by this service at no cost to them.

2) SC officials are monitoring the situation and will after consulting with Experian decide when to go back to the individual identifiers, our focus right now is to protect each effected taxpayer and SC will keep monitoring the call center and until we sure all effected taxpayers are able to register without unreasonable delay we will maintain the current process.

From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Saturday, October 27, 2012 07:58 PM
To: Godfrey, Rob; Stirling, Bryan
Cc: Ken Chaplin <Ken.Chaplin@experianinteractive.com>; Joshua Light <Joshua.Light@experianconsumerdirect.com>; Ken Bixler <Ken.Bixler@experianinteractive.com>; Ozzie Fonseca <ofonseca@experianinteractive.com>
Subject: Rob and Bryan, please review - TIME SENSITIVE

Rob and Bryan,

I am not prepared to answer all of the Post and Courier questions at this point, but here are answers for the ones I feel we can answer. Obviously the paper needs this soon for EOD publishing.

1. Will you be providing your service to everyone in the state who calls and requests it, or just to those who call and you have further reason to believe their identity has been compromised? I'm not sure whether everyone can get it, or whether it just would be for certain people who may be at a higher risk (and whether you have a way of knowing that)? Some woman e-mailed me and said she tried to sign up and was being told she'd have to pay for it. **THE STATE HAS INDICATED THAT SOUTH CAROLINA TAXPAYERS DATING BACK TO 1998 SHOULD REGISTER.**
2. Right now, everyone has to call to get the same code to register for the service online (or you can wait to talk to a customer representative). I'm told on Monday, you'll have unique identifiers for everyone who calls, right? Does that mean you'll have to wait to talk to someone, or will you be able to input your social security number (or some other sort of identifier) to get a code to go online?**THE CURRENT CODE OPOTION IS IN PLACE TO HELP WITH THE TREMENDOUS CALL VOLUME AND PROVIDE A BETTER EXPERIENCE FOR CALLERS. THE INTENT IS TO RETURN TO LIVE SUPPORT FOR ALL CALLERS ONCE THE CALL VOLUME DECREASES.**
3. Some readers e-mailed us and said they tried to register with the code, but the Web site was apparently down. How long has your Web site been unable to process SC residents' requests for protection since this was announced on Friday? **WE ARE NOT AWARE THAT THE WEB SITE HAS NEVER BEEN DOWN AND HAS HAD NO ISSUES ACCEPTING THE CODES, TO THIS POINT.**
4. What else is there we'd like to say? **AT THIS TIME, WE ARE STILL EXPERIENCING ELEVATED CALL VOLUMES, BUT THE CODE OPTION HAS BEEN WELL RECEIVED. WE ENCOURAGE INDIVIDUALS TO USE THE CODE, UNLESS THEY HAVE NO INTERNET ACCESS OR SOME OTHER REASON PREVENTS THEM FROM USING THE**

CODE. IN THAT CASE, THEY SHOULD CALL IN AND TALK TO A LIVE REPRESENTATIVE.

Greg Young
Director, Public Relations
Experian Consumer Services

Godfrey, Rob

From: Courrege, Diette <dcourrege@postandcourier.com>
Sent: Saturday, October 27, 2012 5:05 PM
To: Godfrey, Rob
Subject: FW: update

FYI ... here's what I sent earlier, and I left a message for Jim.

From: Courrege, Diette
Sent: Saturday, October 27, 2012 4:08 PM
To: Godfrey, Rob (RobGodfrey@gov.sc.gov)
Subject: update

Rob,

Thanks again for all of your help today.

Just wanted to give you an update on where I was. I had a long and good conversation with Jim. He provided some really, really consumer-friendly information, and I appreciate you connecting us.

Also, Greg Young from Experion reached out to me via e-mail, and I've submitted questions. I'm waiting on those answers (just sent in the questions a few minutes ago).

The one question that I'm not sure whether Greg is going to answer and Jim couldn't (he didn't remember the #) was the per person dollar figure for the cost of the contract with Experion. Jim said he had that number in his office but didn't have access to today, and he couldn't give me an estimate. Could you?

And I'd like to go ahead and request a copy of the contract the state signed yesterday with Experion. I realize it's Saturday, but if there's anyone who could provide that today, that would be great.

Thanks again.
Diette

Diette Courrege Casey
The Post and Courier
134 Columbus St.
Charleston, S.C. 29403
843.937.5546
843.937.5579 fax
dcourrege@postandcourier.com
http://www.facebook.com/diettecourrege

Godfrey, Rob

From: Harriet McLeod <[redacted]@gmail.com>
Sent: Friday, October 26, 2012 3:53 PM
To: Godfrey, Rob
Subject: Rob, is there a video coming or quotes from the Governor?

Thanks,
Harriet

--
Harriet McLeod
Reuters America
www.reuters.com

Charleston, South Carolina
843-[redacted] (mobile)
[redacted]@gmail.com

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, October 26, 2012 3:55 PM
To: Godfrey, Rob
Subject: RE: For Tim Smith at the Greenville News
Attachments: 4. Cabinet Agency Information Security Policy Highlights.docx

If you're referring to this, I never received this as well... I don't think it was included at all.

Samantha Cheek
Public Information Director
SC Department of Revenue
P.O. Box 125, Columbia, SC 29214
P: 803.898.5281 | F: 803.898.5020
www.sctax.org | Twitter: @SCDOR

From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Friday, October 26, 2012 3:45 PM
To: Samantha Cheek
Subject: For Tim Smith at the Greenville News

Please provide him with the one pager on information security technology that we asked Director Etter to prepare ahead of today's press conference. It was not included in the press kit, and his story says that no report was prepared.

Rob Godfrey
Office of Gov. Nikki Haley
O: (803) 734-5074 | C: (803) 429-5086

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

-###-

Rob Godfrey
Office of Gov. Nikki Haley
O: (803) 734-5074 | C: (803) 429-5086

Thanks,
Graeme Moore
WSPA-TV
864-809-1806

From: Godfrey, Rob [RobGodfrey@gov.sc.gov]
Sent: Friday, October 26, 2012 3:06 PM
Subject: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hacker illegally obtained credit card and Social Security numbers

COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

*****Press kit attached with information regarding the chronology of the investigation and consumer safety solutions is attached.*****

To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Gov. Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1-866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

Godfrey, Rob

From: GMoore@wspa.com
Sent: Friday, October 26, 2012 4:01 PM
To: CheekS@sctax.org
Cc: Godfrey, Rob; WSPA_News@wspa.com
Subject: RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Glad we got that cleared up because from the release it sounds as if you can do either/or.

Also, this is a message we got from a viewer. Thoughts, suggestions?

"Regarding the telephone number in the Revenue Department story, it tells you to call back during business hours 6:00AM to 6:00 PM that it's customer service dept is closed."

Is there an alternate number?

Also, could you reply all?

Thanks,
Graeme

From: Samantha Cheek [CheekS@sctax.org]
Sent: Friday, October 26, 2012 3:58 PM
To: Moore, Graeme C.; RobGodfrey@gov.sc.gov
Subject: RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Graeme,

Taxpayers will need to dial the number provided in order to receive an activation code. They can then sign up via phone or use the activation code online to activate the protection service.

Samantha Cheek
Public Information Director
SC Department of Revenue
P.O. Box 125, Columbia, SC 29214
P: 803.898.5281 | F: 803.898.5020
www.sctax.org | Twitter: @SCDOR

From: GMoore@wspa.com [mailto:GMoore@wspa.com]
Sent: Friday, October 26, 2012 3:40 PM
To: RobGodfrey@gov.sc.gov
Cc: Samantha Cheek
Subject: RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hey Rob and Samantha -
So, I just visited protectmyid.com/scdor -- and I'm stumped. If I am, I know our viewers will be. It says enter an activation code, but one is not provided. Can you provide further? To even try to create an account, you need one of these activation codes. Any clue?

Godfrey, Rob

From: Results@TVEyes-Alerts.com
Sent: Friday, October 26, 2012 4:04 PM
To: Godfrey, Rob
Subject: New MMS Alert - Nikki Haley - WCSC-CHS (CBS)

Media Alert From TVEyes Media Monitoring Suite

(click thumbnail to play)

Nikki Haley on WCSC-CHS (CBS) - Charleston, SC
10/26/2012 16:03:14
Live 5 News First at 4 (News)

... a half million of us have been affected in the state. that news just broke hours ago in columbia. gov. nikki haley and state officials held a news conference to explain the security breach... they say someone in a foreign country gained access to the south carolina department of revenue's website and a server was breached for the first time on august 27th. ...

Content-Language: en-US
X-MS-Has-Attach: yes
X-MS-TNEF-Correlator:
acceptlanguage: en-US
Content-Type: multipart/mixed;
	boundary="_004_B0A6515D1E2B5D48B936DC213B3B8F8E01CA1F7DSCMBXC02bcbadst_"
MIME-Version: 1.0
X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10432:5.7.7855,1.0.431,0.0.0000
 definitions=2012-10-26_05:2012-10-26,2012-10-26,1970-01-01 signatures=0
X-Proofpoint-Spam-Details: rule=notspam policy=default score=0 spamscore=0 suspectscore=0 phishscore=0
 bulkscore=0 adultscore=0 classifier=spam adjust=0 reason=mlx scancount=1
 engine=6.0.2-1203120001 definitions=main-1210260240
To: Undisclosed recipients:;
Return-Path: RobGodfrey@gov.sc.gov

S.C. Department
of Revenue Res...

Godfrey, Rob

From: postmaster@wm.com
To: sesposit@wm.com
Sent: Friday, October 26, 2012 4:05 PM
Subject: Undeliverable: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Delivery has failed to these recipients or distribution lists:

sesposit@wm.com
The recipient's e-mail address was not found in the recipient's e-mail system. Microsoft Exchange will not try to redeliver this message for you. Please check the e-mail address and try resending this message, or provide the following diagnostic text to your system administrator.

Diagnostic information for administrators:

Generating server: wm.com

sesposit@wm.com
#< #5.1.1 smtp;550 5.1.1 RESOLVER.ADR.RecipNotFound; not found> #SMTP#

Original message headers:

Received: from adcpps003.wm.com (192.168.190.102) by ADCHUB003.wm.com
(10.248.35.17) with Microsoft SMTP Server (TLS) id 14.2.283.3; Fri, 26 Oct
2012 15:05:21 -0500
Received: from ciomail2.sc.gov (cioe500.state.sc.us [167.7.36.2]) by
adcpps003.wm.com (8.14.4/8.14.4) with ESMTP id q9QK4u02000830
(version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-SHA bits=256 verify=NOT) for
<sesposit@wm.com>; Fri, 26 Oct 2012 15:04:58 -0500
Received: from (unknown [167.7.136.58]) by ciomail2.sc.gov with smtp (TLS:
TLSv1/SSLv3,128bits,AES128-SHA) id
6f24_6e9b_4873d55c_1fa0_11e2_9528_00188b2fc6a2; Fri, 26 Oct 2012 15:07:33
-0400
Received: from SCMBXC02.bcbad.state.sc.us ([169.254.2.247]) by
sccasht01.bcbad.state.sc.us ([167.7.136.58]) with mapi; Fri, 26 Oct 2012
15:06:29 -0400
From: "Godfrey, Rob" <RobGodfrey@gov.sc.gov>
Date: Fri, 26 Oct 2012 15:06:03 -0400
Subject: S.C. Department of Revenue Responds to Cyber Attack, Will Provide
Credit Monitoring and Identity Theft Protection to Taxpayers
Thread-Topic: S.C. Department of Revenue Responds to Cyber Attack, Will
Provide Credit Monitoring and Identity Theft Protection to Taxpayers
Thread-Index: Ac2zq5SxSUP2i1tBRF2cotd8cilk3A==
Message-ID: <B0A6515D1E2B5D48B936DC213B3B8F8E01CA1F7D@SCMBXC02.bcbad.state.sc.us>
Accept-Language: en-US

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

-###-

Rob Godfrey
Office of Gov. Nikki Haley

O: (803) 734-5074 | C: (803) 429-5086

--

Jonathan Allen
Editor - West Ashley Patch
www.WestAshley.Patch.com
843-608-0092
843-283-9008
facebook.com/pages/West-Ashley-Patch
twitter.com/WestAshleyPatch

On Fri, Oct 26, 2012 at 3:06 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hacker illegally obtained credit card and Social Security numbers

COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

*****Press kit attached with information regarding the chronology of the investigation and consumer safety solutions is attached.*****

To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have happened and what steps to take to address the situation. We also immediately began consultations with state and federal law enforcement agencies and briefed the governor's office."

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Gov. Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1- 866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

Godfrey, Rob

From: Jonathan Allen <jonathan.allen@patch.com>
Sent: Friday, October 26, 2012 4:08 PM
To: Godfrey, Rob
Subject: Re: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Sorry, I've been asked to work on a follow-up to what Sean is writing today. I did not know that had been covered. I will check with him on those questions.

Thanks

On Fri, Oct 26, 2012 at 3:53 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

Y'all had a reporter at this event, and these questions were covered there. Please get with Shawn.

From: Jonathan Allen [mailto:jonathan.allen@patch.com]
Sent: Friday, October 26, 2012 3:52 PM
To: Godfrey, Rob
Subject: Re: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Rob,

Thank you for sending this information along.

I know people will ask, so I'd like to have an explanation for them, why there was a 16-day lag between Oct. 10 when the state first got knowledge of the cyber attack and today when the state issued a statement about it? Did it just take that long to assess the full scale of the attack? Was it not possible to alert state residents sooner that the security of their identities are potentially at risk?

Also the 866 phone number seems to be swamped with recordings telling people to try calling back later, is the state taking measures to increase the staffing on that phone line since 3.6 million residents could potentially be calling it?

Thanks,

--
Jonathan Allen
Editor - West Ashley Patch
www.WestAshley.Patch.com
843-608-0092
843-283-9008
facebook.com/pages/West-Ashley-Patch
twitter.com/WestAshleyPatch

Godfrey, Rob

From: Samantha Cheek <CheekS@sctax.org>
Sent: Friday, October 26, 2012 4:10 PM
To: Godfrey, Rob
Subject: Fwd: Can you jump on a webcam

I don't have access to this, do any of you?

Samantha Cheek
SC Department of Revenue
(803) 898-5281

Begin forwarded message:

> **From:** "Amy Wood" <[redacted]@gmail.com>
> **Date:** October 26, 2012, 4:08:10 PM EDT
> **To:** "CheekS@sctax.org" <CheekS@sctax.org>
> **Subject: Can you jump on a webcam**
>
> I need you for ten minutes to take some viewer questions.
>
> Just takes a laptop with a webcam
>
> Amy Wood
> Interactive New Anchor
> Social TV Instigator
> Innovation Team Champion
> WSPA TV
> 5 6 10 and 11
> (864) 990-3431
> http://About.Me/TVAmyWood
> *warning* messages often dictated via Siri

We are working to get more representatives on the 866 line in order to take taxpayers calls. The number provided is working, however it is just at a high volume at the moment. As time progresses we will be able to identify which taxpayers' confidential numbers were compromised and we will alert those individuals.

Samantha Cheek
Public Information Director
SC Department of Revenue
P.O. Box 125, Columbia, SC 29214
P: 803.898.5281 | F: 803.898.5020
www.sctax.org | Twitter: @SCDOR

From: Beeker, LaDonna [mailto:lbeeker@wistv.com]
Sent: Friday, October 26, 2012 3:18 PM
To: Samantha Cheek
Subject: Public contact info

Hi Samantha,

We are getting a lot of calls complaining about the 866-number not working and/or they can't get through because of "high call volume." Is there more than one phone number available? Or any suggestions for the callers who are getting this recording? Is the DOR working on anything else to get the public in touch with a person to find out if they have been compromised?

Please advise of any info we can give the viewers as they call and as we are coming up on future broadcasts. Thanks for your help.

LaDonna Beeker
Investigative producer
WIS-TV
803-309-6518
lbeeker@wistv.com-

Godfrey, Rob

From: Gatson, Judi <jgatson@wistv.com>
Sent: Friday, October 26, 2012 4:17 PM
To: Samantha Cheek
Cc: Norman, Meaghan; Godfrey, Rob
Subject: Re: Number info - from SCDOR

Any idea why viewers are getting a recording saying the call center is closed?

~ jg

On Oct 26, 2012, at 4:15 PM, "Samantha Cheek" <CheekS@sctax.org> wrote:

> We're unsure as to those details – the call center is open and available for taxpayers to call 24/7.
>
> Samantha Cheek
> Public Information Director
> SC Department of Revenue
> P.O. Box 125, Columbia, SC 29214
> P: 803.898.5281 | F: 803.898.5020
> www.sctax.org | Twitter: @SCDOR
>
> **From:** Gatson, Judi [mailto:jgatson@wistv.com]
> **Sent:** Friday, October 26, 2012 3:31 PM
> **To:** Samantha Cheek
> **Cc:** Norman, Meaghan
> **Subject:** Fwd: Number info - from SCDOR
>
> Samantha,
>
> How many operators are currently working that phone line? How many operators do you hope to add? Where is the call center located? And Is the line open 24 hours a day?
>
> Many thx,
> ~ jg
>
> Begin forwarded message:
>
> > **From:** "Beeker, LaDonna" <lbeeker@wistv.com>
> > **Date:** October 26, 2012, 3:29:25 PM EDT
> > **To:** All WIS Producers <AllWISProducers@wistv.com>
> > **Subject: Number info - from SCDOR**
> >
> > Just got this ...
> >
> > **From:** Samantha Cheek [mailto:CheekS@sctax.org]
> > **Sent:** Friday, October 26, 2012 3:29 PM
> > **To:** Beeker, LaDonna
> > **Subject:** RE: Public contact info

Upon the recommendation of law enforcement officials, DOR contracted Mandiant, one of the world's top information security companies, to assist in the investigation, help secure the system, install new equipment and software and institute tighter controls on access.

On October 16, investigators uncovered two attempts to probe the system in early September, and later learned that a previous attempt was made in late August. In mid-September, two other intrusions occurred, and to the best of the department's knowledge, the hacker obtained data for the first time. No other intrusions have been uncovered at this time. On October 20, the vulnerability in the system was closed and, to the best of the department's knowledge, secured.

"The number of records breached requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens," said Governor Nikki Haley. "We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring and identity protection to those affected."

Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or call 1-866-578-5422 to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of identity protection service provided by Experian.

Experian's ProtectMyID™ Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus. The alerts and daily monitoring services are provided for one year, and consumers will continue to have access to fraud resolution agents and services beyond the first year.

In addition to the Experian service, state officials urged individuals to consider additional steps to protect their identity and financial information, including:

- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

If credit card information is compromised, the best protection is to have the bank reissue the card. Anyone who has used a credit card in a transaction with the Department of Revenue should check bank accounts regularly to see if any unauthorized charges have occurred. If so, the cardholder should contact the credit card issuer immediately by calling the toll-free number located on the back of the card or on a monthly statement, tell them what you have seen, and ask them to cancel and reissue the card. Consumers should also change any credit card web account passwords immediately when unauthorized charges are detected.

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."

###