

Pitts, Ted

From: Schimsa, Rebecca
Sent: Thursday, November 01, 2012 7:16 PM
To: Stirling, Bryan
Cc: Patel, Swati; Pitts, Ted
Subject: Fw: SCANA insert
Attachments: SCANA.docx

Please approve. Tomorrow, I will disseminate to SCANA.

From: Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
Sent: Thursday, November 01, 2012 05:46 PM
To: Schimsa, Rebecca
Cc: Rick Silver <Rick.Silver@chernoffnewman.com>; Emily Brady <Emily.Brady@chernoffnewman.com>
Subject: SCANA insert

Rebecca, the copy for the SCANA insert is attached. It comes in at just under 800 characters and is language that has all been approved by staff and lawyers in other formats. If you have any questions, please contact me. Thank you for your help.



Tim Kelly
Public Relations Strategist
Chernoff Newman
e: tim.kelly@chernoffnewman.com
w: www.chernoffnewman.com
me: <https://www.vizify.com/tim-kelly>
p: 803.233.2459

1411 Gervais Street
Columbia, SC 29201



Follow Chernoff Newman

Pitts, Ted

From: Patel, Swati
Sent: Tuesday, January 08, 2013 9:09 AM
To: Pitts, Ted
Subject: FW: Chernoff Newman Contract
Attachments: Chernoff Newman-NMRS Agency Service Agreement - 4819-8971-9314 v 1.pdf;
Chernoff Newman-NMRS NonDisclosure Agreement - 4852-4436-8146 v 1.pdf

Here are the executed agreements.

From: Jessica Trautman [mailto:jessica.trautman@nelsonmullins.com] **On Behalf Of** Rush Smith
Sent: Monday, January 07, 2013 10:36 AM
To: Patel, Swati; kimpsom@sctax.org
Cc: Thad Westbrook; Diane Argabright; Rush Smith
Subject: RE: Chernoff Newman Contract

Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com
Nelson Mullins Riley & Scarborough, LLP, Columbia SC

From: "Patel, Swati" <SwatiPatel@gov.sc.gov>
Date: January 7, 2013, 10:08:21 AM EST
To: Rush Smith <rush.smith@nelsonmullins.com>, "Thad H. Westbrook (thad.westbrook@nelsonmullins.com) (thad.westbrook@nelsonmullins.com)" <thad.westbrook@nelsonmullins.com>, "'Jon Neiditz' (Jon.Neiditz@nelsonmullins.com)" <Jon.Neiditz@nelsonmullins.com>
Cc: "Pitts, Ted" <TedPitts@gov.sc.gov>, "kimpsom@sctax.org" <kimpsom@sctax.org>
Subject: Chernoff Newman Contract

Rush,
Can you please send us and Milton the executed Chernoff Newman contract asap. We have the contract that is signed by Chernoff only.

Thanks,
Swati

From: Pitts, Ted
Sent: Monday, January 07, 2013 9:46 AM
To: Patel, Swati
Subject: FW: Chernoff Newman Contract

From: Lisa Catalanotto [mailto:LisaCatalanotto@scsenate.gov]
Sent: Friday, January 04, 2013 4:51 PM
To: Pitts, Ted
Subject: Chernoff Newman Contract

Pitts, Ted

From: Jenny Renedo <RENEDOJ@sctax.org>
Sent: Tuesday, January 08, 2013 2:43 PM
To: Butch.Bowers@wcsr.com; Pitts, Ted
Subject: phone call with Bill Blume today at 3:00

Bill would like to have a conference call with you both at 3:00. Butch, I have your number as 454-7720. Ted, I have 767-7862 as your number. Please correct me if he should use a different number.

Please and thank you

Jenny Renedo, 898-5148
Administrative Coordinator
Office of the Director
SC Department of Revenue

Pitts, Ted

From: Patel, Swati
Sent: Thursday, January 03, 2013 11:39 AM
To: Pitts, Ted
Subject: FW: Executed Contracts and Confidentiality Agreement
Attachments: DOR Contracts with SourceLink.pdf

From: Milton Kimpson [mailto:KimpsoM@sctax.org]
Sent: Friday, November 30, 2012 4:07 PM
To: nhendley@sourcelink.com
Cc: Patel, Swati; WattsL@sctax.org; Jaquetta Campbell Wright
Subject: Executed Contracts and Confidentiality Agreement

Noel:

Please find contracts signed by the Department. If someone would sign on behalf of SourceLink and send fully executed back by e-mail. Thanks

Milton

Milton G. Kimpson
General Counsel for Litigation
South Carolina Department of Revenue
P.O. Box 12265
Columbia, SC 29211
803-898-5131
803-898-5147 (fax)

Pitts, Ted

From: Jon Neiditz <Jon.Neiditz@nelsonmullins.com>
Sent: Thursday, January 03, 2013 10:51 AM
To: Pitts, Ted
Cc: Rush Smith
Subject: Re: Why Experian?

10/23.

Sent from my iPhone

On Jan 3, 2013, at 10:40 AM, "Pitts, Ted" <TedPitts@gov.sc.gov> wrote:

John,

What was the date you first contacted Experian about services in response to the DOR situation?

Thanks.

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

From: Jon Neiditz [<mailto:Jon.Neiditz@nelsonmullins.com>]
Sent: Tuesday, December 18, 2012 5:31 PM
To: Milton Kimpson (KimpsoM@sctax.org); Patel, Swati; Rush Smith; Pitts, Ted; Thad Westbrook
Subject: Why Experian?

1. SSN breaches (unlike credit cards or other things that can be changed) require a monitoring service as well as resolution services.
2. The only monitoring service that is publically understood (because not proprietary) and generally demonstrated to be effective (and recognized by regulators as such) in the context of SSN breaches is credit monitoring.
3. There are many innovative monitoring services other than credit monitoring, but because of their proprietary methods, they are more like "black boxes," and therefore harder to explain, perhaps less reliable, less accountable and riskier in a very high-profile and controversial breach such as this one.
4. Many of these innovative vendors also do not have the size, resources and capacity for quick response of the largest breach response vendors.
5. Therefore, credit monitoring is the right choice as a monitoring service for this SSN breach.
6. Once you choose credit monitoring, there are only three credit bureaus that have direct access to credit bureau information; all other vendors have to buy the information from the credit bureaus, adding to cost and decreasing efficiency and accountability.

7. Of the three credit bureaus, Experian does far more credit monitoring than the others and has the most mature and reliable products available for the lowest prices, in addition to being the largest bureau and having the capacity to respond the most quickly.
8. Experian also offered resolution services that don't expire for adults as part of its monitoring product, and included an insurance policy that covers not only ID theft but electronic fund transfers, mitigating the exposure from breached bank account numbers.

Confidentiality Notice

This message is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged, confidential or otherwise legally exempt from disclosure.

If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately either by phone (800-237-2000) or reply to this e-mail and delete all copies of this message.

To ensure compliance with the requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including the attachments) is not intended or written to be used, for the purpose of (a) avoiding penalties under the Internal Revenue Code or (b) promoting, marketing or recommending to another party any transaction or tax-related matter[s]. To provide you with a communication that could be used to avoid penalties under the Internal Revenue Code will necessarily entail additional investigations, analysis and conclusions on our part.

Pitts, Ted

From: Schimsa, Rebecca
Sent: Thursday, January 03, 2013 10:28 AM
To: Pitts, Ted
Subject: FW: Cabinet response to IT security after DOR
Attachments: Cabinet response to IT security after DOR.doc

From: Pitts, Ted
Sent: Wednesday, November 14, 2012 9:35 AM
To: Schimsa, Rebecca; Veldran, Katherine
Subject: Cabinet response to IT security after DOR

Pitts, Ted

From: Jon Neiditz <Jon.Neiditz@nelsonmullins.com>
Sent: Tuesday, December 18, 2012 6:45 PM
To: Milton Kimpson (KimpsoM@sctax.org); Patel, Swati; Rush Smith; Pitts, Ted; Thad Westbrook
Subject: RE: Why Experian?

Just to follow up, I can verify that the statement mentioned by Ted that participation percentages in credit monitoring are generally lower in very large breaches is indeed a common expectation with considerable basis in fact (except in this case).

From: Jon Neiditz
Sent: Tuesday, December 18, 2012 5:31 PM
To: Milton Kimpson (KimpsoM@sctax.org); Swati Patel (swatipatel@gov.sc.gov); Rush Smith; Pitts, Ted (TedPitts@gov.sc.gov); Thad Westbrook
Subject: Why Experian?

1. SSN breaches (unlike credit cards or other things that can be changed) require a monitoring service as well as resolution services.
2. The only monitoring service that is publically understood (because not proprietary) and generally demonstrated to be effective (and recognized by regulators as such) in the context of SSN breaches is credit monitoring.
3. There are many innovative monitoring services other than credit monitoring, but because of their proprietary methods, they are more like "black boxes," and therefore harder to explain, perhaps less reliable, less accountable and riskier in a very high-profile and controversial breach such as this one.
4. Many of these innovative vendors also do not have the size, resources and capacity for quick response of the largest breach response vendors.
5. Therefore, credit monitoring is the right choice as a monitoring service for this SSN breach.
6. Once you choose credit monitoring, there are only three credit bureaus that have direct access to credit bureau information; all other vendors have to buy the information from the credit bureaus, adding to cost and decreasing efficiency and accountability.
7. Of the three credit bureaus, Experian does far more credit monitoring than the others and has the most mature and reliable products available for the lowest prices, in addition to being the largest bureau and having the capacity to respond the most quickly.
8. Experian also offered resolution services that don't expire for adults as part of its monitoring product, and included an insurance policy that covers not only ID theft but electronic fund transfers, mitigating the exposure from breached bank account numbers.

Confidentiality Notice

This message is intended exclusively for the individual or entity to which it is addressed. This communication may contain information that is proprietary, privileged, confidential or otherwise legally exempt from disclosure.

If you are not the named addressee, you are not authorized to read, print, retain, copy or disseminate this message or any part of it. If you have received this message in error, please notify the sender immediately either by phone (800-237-2000) or reply to this e-mail and delete all copies of this message.

Pitts, Ted

From: Rush Smith <rush.smith@nelsonmullins.com>
Sent: Friday, October 26, 2012 2:25 PM
To: ofonseca@experianinteractive.com
Cc: jon.neiditz@nelsonmullins.com; KimpsoM@sctax.org;
thad.westbrook@nelsonmullins.com; Emily.Brady@chernoffnewman.com;
Rick.Silver@chernoffnewman.com; Tim.Kelly@chernoffnewman.com; Pitts, Ted; Stirling,
Bryan; Harry T. Cooper Jr. Esquire
Subject: Re: Experian

Ozzie,

We have finished press conference and local news media are continuing live with the story. I wanted to let you know.
Rush

Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com
Nelson Mullins Riley & Scarborough, LLP, Columbia SC

Sent from my iPad

On Oct 26, 2012, at 1:35 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> Thank you. Please keep us posted.

>

> ----- Original Message -----

> From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]

> Sent: Friday, October 26, 2012 01:34 PM

> To: Rush Smith <rush.smith@nelsonmullins.com>

> Cc: Ozzie Fonseca <ofonseca@experianinteractive.com>; Jon Neiditz

> <jon.neiditz@nelsonmullins.com>; KimpsoM@sctax.org

> <KimpsoM@sctax.org>; Thad Westbrook

> <thad.westbrook@nelsonmullins.com>; Stirling, Bryan; Emily Brady

> <Emily.Brady@chernoffnewman.com>; Rick Silver

> <Rick.Silver@chernoffnewman.com>; Tim Kelly

> <Tim.Kelly@chernoffnewman.com>; Pitts, Ted

> Subject: Re: Experian

>

> On the phone with our call center management. Additional staffing will be allocated as appropriate.

>

> Current hold time is now 5 minutes and dropping.

>

> Ozzie Fonseca, CIPP/US

> Senior Director, Data Breach Resolution

>

> Experian Consumer Direct

> 535 Anton, Suite 100.

> Costa Mesa, CA 92626

> (949) 567-3851 - Desk

> (949) 302-2299 -

> Cell (949) 242-2938 - Fax

> ozzie.fonseca@experian.com<mailto:ozzie.fonseca@experian.com>
>
> Blog:
> www.Experian.com/blogs/data-breach<<http://www.Experian.com/blogs/data-breach>> Follow us on Twitter:
> www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR>
> Visit us at <http://www.experian.com/databreach>
>
> CONFIDENTIALITY NOTICE: This email message and any accompanying data or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the email address above, delete this email from your computer, and destroy any copies in any form immediately. Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other applicable privilege.
>
>
> Rush Smith <rush.smith@nelsonmullins.com> wrote:
>
> Ozzie?
>
> Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com Nelson
> Mullins Riley & Scarborough, LLP, Columbia SC
>
> Sent from my iPad
>
> On Oct 26, 2012, at 1:29 PM, "Pitts, Ted" <TedPitts@gov.sc.gov> wrote:
>
>> Called the 866 number am on the phone with rep now wait time was 8 minutes 19 seconds.
>>
>> Ted
>>
>> -----Original Message-----
>> From: Rush Smith [<mailto:rush.smith@nelsonmullins.com>]
>> Sent: Friday, October 26, 2012 1:27 PM
>> To: Ozzie Fonseca
>> Cc: Jon Neiditz; KimpsoM@sctax.org; Thad Westbrook; Stirling, Bryan;
>> Pitts, Ted; Emily Brady; Rick Silver; Tim Kelly
>> Subject: Re: Experian
>>
>> Ozzie,
>> We need some content on the website ASAP so that we can have a happier consumer experience. It should tell people to call the number, get a code, and the return to the website to enroll. Please get that added. Thanks much.
>> Rush
>>
>> Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com Nelson
>> Mullins Riley & Scarborough, LLP, Columbia SC
>>
>> Sent from my iPad
>>
>> On Oct 26, 2012, at 12:58 PM, "Ozzie Fonseca" <ofonseca@experianinteractive.com> wrote:
>>

>>> I just hung up with our call center. They are getting calls already and I are distributing codes to those were interested.

>>>

>>> Given the fact that we are already taking calls I am a little concerned by not having enough codes to assign to each individual.

>>>

>>> If you decide that 3.6 million is the right number we will do our best, but in the interest of the best customer experience I would suggest ordering the correct amount. Otherwise, we should create a short addendum to request additional codes later today.

>>>

>>> Please let me know your thoughts.

>>>

>>> Ozzie Fonseca, CIPP/US

>>> Senior Director, Data Breach Resolution

>>>

>>> Experian Consumer Direct

>>> 535 Anton, Suite 100.

>>> Costa Mesa, CA 92626

>>> (949) 567-3851 - Desk

>>> (949) 302-2299 -

>>> Cell (949) 242-2938 - Fax

>>> ozzie.fonseca@experian.com<mailto:ozzie.fonseca@experian.com>

>>>

>>> Blog:

>>> www.Experian.com/blogs/data-breach<<http://www.Experian.com/blogs/data-breach>>

>>> a-<<http://www.Experian.com/blogs/data-breach>>

>>> /blogs/data->

>>> breach> Follow us on Twitter:

>>> www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR>

>>> p://www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR>

>>> >> Visit us at <http://www.experian.com/databreach>

>>>

>>> CONFIDENTIALITY NOTICE: This email message and any accompanying data or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the email address above, delete this email from your computer, and destroy any copies in any form immediately. Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other applicable privilege.

>>>

>>>

>>> Rush Smith <rush.smith@nelsonmullins.com> wrote:

>>>

>>> Can you give us guidance on this? Story broke and you will start

>>> getting calls. Is call center ready? Please let us know when it

>>> will be. You should have signed contract soon.

>>>

>>> Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com Nelson

>>> Mullins Riley & Scarborough, LLP, Columbia SC

>>>

>>>

>>>

>>> -----Original Message-----

>>> From: Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
>>> Sent: Friday, October 26, 2012 12:52 PM
>>> To: Rush Smith
>>> Subject: Experian
>>>
>>> People are going to site and being asked to enter a code.
>>>
>>> Sent from my iPhone
>
>

Pitts, Ted

From: Rush Smith <rush.smith@nelsonmullins.com>
Sent: Friday, October 26, 2012 8:31 AM
To: Pitts, Ted
Cc: Thad H. Westbrook
Subject: Just checking in about proposed contract

Please let me know if there have been any other developments regarding execution of contract.

I think you have my cell but in case you don't it is 803-██████████.

Thanks.

Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com
Nelson Mullins Riley & Scarborough, LLP, Columbia SC

Sent from my iPhone

Pitts, Ted

To: Rush Smith
Subject: RE: Just checking in about proposed contract

Rush

-----Original Message-----

From: Rush Smith [mailto:rush.smith@nelsonmullins.com]
Sent: Friday, October 26, 2012 8:31 AM
To: Pitts, Ted
Cc: Thad H. Westbrook
Subject: Just checking in about proposed contract

Please let me know if there have been any other developments regarding execution of contract.

I think you have my cell but in case you don't it is 803-606-1406.

Thanks.

Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com
Nelson Mullins Riley & Scarborough, LLP, Columbia SC

Sent from my iPhone

Pitts, Ted

From: Schimsa, Rebecca
Sent: Friday, October 26, 2012 7:19 PM
To: 'Istavrinakis@msn.com'
Cc: Pitts, Ted; Veldran, Katherine
Subject: Re: From the Governor's Office re. cyber-attack at DOR

Thank you for your questions, Representative. I understand that our Chief of Staff, Bryan Stirling, has reached out to you.

If you have any further questions, please let Bryan know.

From: Leon Stavrinakis [mailto:Istavrinakis@msn.com]
Sent: Friday, October 26, 2012 06:32 PM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine
Subject: Re: From the Governor's Office re. cyber-attack at DOR

How will you control access to this conf call now that the time and number have been published in the media?

Representative Leon Stavrinakis
Stavrinakis Law Firm
843-813-2800
leon@stavlaw.net
leonstav@schouse.gov

On Oct 26, 2012, at 4:44 PM, "Schimsa, Rebecca" <RebeccaSchimsa@gov.sc.gov> wrote:

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

In regards to the cyber-attack at the Department of Revenue announced this afternoon, we are sending you the following information: (1) the media release from our office (below); (2) the media release from the Department of Revenue (attached); (3) a link to the video of today's press conference; and (4) an invitation to a conference call on Monday morning with Chief Keel, Director Etter, and Inspector General Maley (below).

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

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.

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 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.”

-###-

VIDEO OF TODAY’S PRESS CONFERENCE:

The S.C. Department of Revenue announced on October 26, 2012 that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack.

Governor Nikki Haley, South Carolina Law Enforcement Division Chief Mark Keel, United States Secret Service Special Agent in Charge Michael Williams, South Carolina Department of Revenue Director Jim Etter and State Inspector General Patrick Maley today responded to news of the cyber attack with consumer safety solutions during an afternoon press conference.

Video of the press conference is available here: <http://www.youtube.com/watch?v=0Dax66JEzVs&>
Attached you will find a press kit that includes consumer safety solutions.

Anyone who has filed a South Carolina tax return since 1998 should take the following steps:

1. Call 1-866-578-5422 where you will 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.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit <http://www.protectmyid.com/scdor>. For the US Mail service, you will receive notifications via the US mail.

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.

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

Our office has arranged a conference call for members of the General Assembly to be held on Monday, October 29th at 10:00 a.m. with Chief Mark Keel, Director Jim Etter, and Inspector General Pat Maley. The purpose of the conference call is to give you the opportunity to receive information and ask questions about the cyber-attack at the Department of Revenue. There is a limited number of lines available. This call is only intended for you, members of the General Assembly, or a staff member calling in on your behalf.

Call Number: 1-800-670-1742 (No access code is needed.)

Directions:

1. Upon dialing the conference number, each participant will be asked his or her name and then be placed into the conference call.
2. Participants should plan to join the call 5-10 minutes prior to the start of the call.
3. Once the speakers have completed their statements, the call operator will provide instructions for the question and answer portion of the call.
4. All participants will be given the opportunity to ask questions.
5. Questions will be announced in the order that they are received.
6. For operator assistance at any time during the call, please press *0.

-###-

<Media Release from DOR 10.26.2012.pdf>

Pitts, Ted

From: Leon Stavrinakis <lstavrinakis@msn.com>
Sent: Friday, October 26, 2012 10:29 PM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine
Subject: RE: From the Governor's Office re. cyber-attack at DOR

He did. Thank you all very much for the prompt reply.

Leon E. Stavrinakis / Attorney at Law / Stavrinakis Law Firm
S.C. House of Representatives / District 119, Charleston County
One Cool Blow Street, Suite 201 / Charleston, SC 29403
843.724.1060 (Law Office) / 843.853.7816 (Law Fax)
803.734.3039 (State House Office) / 888.626.9708 (E-Fax)
stavlaw.net / leonforhouse.com

This message (including any attachments) is intended solely for the use of the individual(s) to whom it is addressed and may contain information that is privileged, confidential or otherwise exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution, or copying of this communication is strictly prohibited. If you have received this communication in error, please immediately reply to this message or notify us by telephone at 843-724-1060 and delete the message. Thank you.

From: RebeccaSchimsa@gov.sc.gov
To: lstavrinakis@msn.com
CC: TedPitts@gov.sc.gov; KatherineVeldran@gov.sc.gov
Date: Fri, 26 Oct 2012 19:19:16 -0400
Subject: Re: From the Governor's Office re. cyber-attack at DOR

Thank you for your questions, Representative. I understand that our Chief of Staff, Bryan Stirling, has reached out to you.

If you have any further questions, please let Bryan know.

From: Leon Stavrinakis [mailto:lstavrinakis@msn.com]
Sent: Friday, October 26, 2012 06:32 PM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine
Subject: Re: From the Governor's Office re. cyber-attack at DOR

How will you control access to this conf call now that the time and number have been published in the media?

Representative Leon Stavrinakis
Stavrinakis Law Firm
843-813-2800

On Oct 26, 2012, at 4:44 PM, "Schimsa, Rebecca" <RebeccaSchimsa@gov.sc.gov> wrote:

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

In regards to the cyber-attack at the Department of Revenue announced this afternoon, we are sending you the following information: (1) the media release from our office (below); (2) the media release from the Department of Revenue (attached); (3) a link to the video of today's press conference; and (4) an invitation to a conference call on Monday morning with Chief Keel, Director Etter, and Inspector General Maley (below).

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

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.

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 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."

-###-

VIDEO OF TODAY'S PRESS CONFERENCE:

The S.C. Department of Revenue announced on October 26, 2012 that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed

in a cyber attack.

Governor Nikki Haley, South Carolina Law Enforcement Division Chief Mark Keel, United States Secret Service Special Agent in Charge Michael Williams, South Carolina Department of Revenue Director Jim Etter and State Inspector General Patrick Maley today responded to news of the cyber attack with consumer safety solutions during an afternoon press conference.

Video of the press conference is available here:

<http://www.youtube.com/watch?v=0Dax66JEzVs> Attached you will find a press kit that includes consumer safety solutions.

Anyone who has filed a South Carolina tax return since 1998 should take the following steps:

1. Call 1-866-578-5422 where you will 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.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit <http://www.protectmyid.com/scdor>. For the US Mail service, you will receive notifications via the US mail.

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.

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

Our office has arranged a conference call for members of the General Assembly to be held on Monday, October 29th at 10:00 a.m. with Chief Mark Keel, Director Jim Etter, and Inspector General Pat Maley. The purpose of the conference call is to give you the opportunity to receive information and ask questions about the cyber-attack at the Department of Revenue. There is a limited number of lines available. This call is only intended for you, members of the General Assembly, or a staff member calling in on your behalf.

Call Number: 1-800-670-1742 (No access code is needed.)

Directions:

1. Upon dialing the conference number, each participant will be asked his or her name and then be placed into the conference call.
2. Participants should plan to join the call 5-10 minutes prior to the start of the call.
3. Once the speakers have completed their statements, the call operator will provide instructions for the question and answer portion of the call.
4. All participants will be given the opportunity to ask questions.
5. Questions will be announced in the order that they are received.

6. For operator assistance at any time during the call, please press *0.

-###-

<Media Release from DOR 10.26.2012.pdf>

Pitts, Ted

From: Tim Kelly <Tim.Kelly@chernoffnewman.com>
Sent: Friday, October 26, 2012 3:13 PM
To: Ozzie Fonseca; Jon Neiditz
Cc: Rush Smith; Pitts, Ted; Stirling, Bryan; Harry T. Cooper Jr. Esquire
Subject: RE: Experian

The current message on the number is stating that the call center is closed.

-----Original Message-----

From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 2:51 PM
To: Jon Neiditz
Cc: Rush Smith; Ozzie Fonseca; KimpsoM@sctax.org; Thad Westbrook; Emily Brady; Rick Silver; Tim Kelly; Pitts, Ted; Stirling, Bryan; Harry T. Cooper Jr. Esquire
Subject: RE: Experian

Jon:

And FAQ regarding minors would certainly be useful. We have received a few calls regarding children.

Thanks

Ozzie Fonseca, CIPP/US
Senior Director, Data Breach Resolution

Experian Consumer Direct
535 Anton, Suite 100.
Costa Mesa, CA 92626
(949) 567-3851 - Desk
(949) 302-2299 -
Cell (949) 242-2938 - Fax
ozzie.fonseca@experian.com<mailto:ozzie.fonseca@experian.com>

Blog:
www.Experian.com/blogs/data-breach<[http://www.Experian.com/blogs/data-br](http://www.Experian.com/blogs/data-breach)
each>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR>
Visit us at <http://www.experian.com/databreach>

CONFIDENTIALITY NOTICE: This email message and any accompanying data or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the email address above, delete this email from your computer, and destroy any copies in any form immediately.

Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other applicable privilege.

Jon Neiditz <Jon.Neiditz@nelsonmullins.com> wrote:

Hats off to Jim Etter, the calming voice in the storm. Ozzie, the reporters (in addition to telling everyone the state has probably paid \$50 per enrollee, and calculating that out at 100% participation) have suggested that children should be enrolled. Do you have or need an FAQ on the likelihood of children's SSNs being included in the records?

Jon A. Neiditz
Partner
jon.neiditz@nelsonmullins.com
Nelson Mullins Riley & Scarborough LLP
Atlantic Station
201 17th Street NW, Suite 1700
Atlanta, GA 30363
Tel: 404.322.6139 Fax: 404.322.6033
<http://www.nelsonmullins.com/attorneys/jon-neiditz>

-----Original Message-----

From: Rush Smith
Sent: Friday, October 26, 2012 2:25 PM
To: ofonseca@experianinteractive.com
Cc: Jon Neiditz; KimpsoM@sctax.org; Thad Westbrook; Emily.Brady@chernoffnewman.com; Rick.Silver@chernoffnewman.com; Tim.Kelly@chernoffnewman.com; Pitts, Ted; Stirling, Bryan; Harry T. Cooper Jr. Esquire
Subject: Re: Experian

Ozzie,
We have finished press conference and local news media are continuing live with the story. I wanted to let you know.
Rush

Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com

Nelson Mullins Riley & Scarborough, LLP, Columbia SC

Sent from my iPad

On Oct 26, 2012, at 1:35 PM, "Stirling, Bryan"
<BryanStirling@gov.sc.gov> wrote:

> Thank you. Please keep us posted.

>

> ----- Original Message -----

> From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]

> Sent: Friday, October 26, 2012 01:34 PM

> To: Rush Smith <rush.smith@nelsonmullins.com>

> Cc: Ozzie Fonseca <ofonseca@experianinteractive.com>; Jon Neiditz

> <jon.neiditz@nelsonmullins.com>; KimpsoM@sctax.org

> <KimpsoM@sctax.org>; Thad Westbrook

> <thad.westbrook@nelsonmullins.com>; Stirling, Bryan; Emily Brady
> <Emily.Brady@chernoffnewman.com>; Rick Silver
> <Rick.Silver@chernoffnewman.com>; Tim Kelly
> <Tim.Kelly@chernoffnewman.com>; Pitts, Ted
> Subject: Re: Experian
>
> On the phone with our call center management. Additional staffing
will be allocated as appropriate.
>
> Current hold time is now 5 minutes and dropping.
>
> Ozzie Fonseca, CIPP/US
> Senior Director, Data Breach Resolution
>
> Experian Consumer Direct
> 535 Anton, Suite 100.
> Costa Mesa, CA 92626
> (949) 567-3851 - Desk
> (949) 302-2299 -
> Cell (949) 242-2938 - Fax
> ozzie.fonseca@experian.com<mailto:ozzie.fonseca@experian.com>
>
> Blog:
> www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-
> <http://www.Experian.com/blogs/data-breach<http://www.Experian.com/blo
> gs/data->
> breach> Follow us on Twitter:
> www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR<http:
> //www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR>>
> Visit us at http://www.experian.com/databreach
>
> CONFIDENTIALITY NOTICE: This email message and any accompanying data
or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not
the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is
strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the
email address above, delete this email from your computer, and destroy any copies in any form immediately.
Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other
applicable privilege.
>
>
> Rush Smith <rush.smith@nelsonmullins.com> wrote:
>
> Ozzie?
>
> Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com Nelson
> Mullins Riley & Scarborough, LLP, Columbia SC
>
> Sent from my iPad
>
> On Oct 26, 2012, at 1:29 PM, "Pitts, Ted" <TedPitts@gov.sc.gov> wrote:
>
>> Called the 866 number am on the phone with rep now wait time was 8

minutes 19 seconds.

>>

>> Ted

>>

>> -----Original Message-----

>> From: Rush Smith [mailto:rush.smith@nelsonmullins.com]

>> Sent: Friday, October 26, 2012 1:27 PM

>> To: Ozzie Fonseca

>> Cc: Jon Neiditz; KimpsoM@sctax.org; Thad Westbrook; Stirling, Bryan;

>> Pitts, Ted; Emily Brady; Rick Silver; Tim Kelly

>> Subject: Re: Experian

>>

>> Ozzie,

>> We need some content on the website ASAP so that we can have a happier consumer experience. It should tell people to call the number, get a code, and then return to the website to enroll. Please get that added. Thanks much.

>> Rush

>>

>> Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com Nelson

>> Mullins Riley & Scarborough, LLP, Columbia SC

>>

>> Sent from my iPad

>>

>> On Oct 26, 2012, at 12:58 PM, "Ozzie Fonseca"

<ofonseca@experianinteractive.com> wrote:

>>

>>> I just hung up with our call center. They are getting calls already and I am distributing codes to those who were interested.

>>>

>>> Given the fact that we are already taking calls I am a little concerned by not having enough codes to assign to each individual.

>>>

>>> If you decide that 3.6 million is the right number we will do our best, but in the interest of the best customer experience I would suggest ordering the correct amount. Otherwise, we should create a short addendum to request additional codes later today.

>>>

>>> Please let me know your thoughts.

>>>

>>> Ozzie Fonseca, CIPP/US

>>> Senior Director, Data Breach Resolution

>>>

>>> Experian Consumer Direct

>>> 535 Anton, Suite 100.

>>> Costa Mesa, CA 92626

>>> (949) 567-3851 - Desk

>>> (949) 302-2299 -

>>> Cell (949) 242-2938 - Fax

>>> ozzie.fonseca@experian.com<mailto:ozzie.fonseca@experian.com>

>>>

>>> Blog:

>>> www.Experian.com/blogs/data-breach<<http://www.Experian.com/blogs/data-breach>>

>>> <<http://www.Experian.com/blogs/data-breach>><<http://www.Experian.com/blogs/data-breach>>

>>> logs/dat>
>>> a-<http://www.Experian.com/blogs/data-breach<http://www.Experian.com
>>> /blogs/data->
>>> breach> Follow us on Twitter:
>>> www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR<htt
>>> <http://www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian
>>> _DBR<htt>
>>> p://www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR
>>> >> Visit us at http://www.experian.com/databreach
>>>
>>> CONFIDENTIALITY NOTICE: This email message and any accompanying data
or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not
the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is
strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the
email address above, delete this email from your computer, and destroy any copies in any form immediately.
Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other
applicable privilege.
>>>
>>>
>>> Rush Smith <rush.smith@nelsonmullins.com> wrote:
>>>
>>> Can you give us guidance on this? Story broke and you will start
>>> getting calls. Is call center ready? Please let us know when it
>>> will be. You should have signed contract soon.
>>>
>>> Rush Smith | 803-255-9492 | rush.smith@nelsonmullins.com Nelson
>>> Mullins Riley & Scarborough, LLP, Columbia SC
>>>
>>>
>>>
>>> -----Original Message-----
>>> From: Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
>>> Sent: Friday, October 26, 2012 12:52 PM
>>> To: Rush Smith
>>> Subject: Experian
>>>
>>> People are going to site and being asked to enter a code.
>>>
>>> Sent from my iPhone
>
>

Pitts, Ted

From: Thad Westbrook <thad.westbrook@nelsonmullins.com>
Sent: Monday, November 26, 2012 9:09 AM
To: Marshall Heilman
Cc: Pitts, Ted; Jon Neiditz; Rush Smith; Butch.Bowers@wcsr.com; TClaypoole@wcsr.com
Subject: SC Senate Hearing

Marshall,

The SC Senate has a study committee that is investigating the data breach at the SC Department of Revenue. Ted Pitts informed us a few minutes ago that the committee would like for you to appear on Wednesday and testify during the hearing. Therefore, Ted Pitts will call you to discuss the committee's request and your schedule.

Let us know if you have any questions.

Thank you,
Thad

Nelson Mullins

Thad H. Westbrook

Partner
thad.westbrook@nelsonmullins.com

Nelson Mullins Riley & Scarborough LLP

Meridian, 17th Floor
1320 Main Street, Columbia, SC 29201
Tel: 803.255.5568 Fax: 803.255.9088

www.nelsonmullins.com
([View Bio](#))

Pitts, Ted

From: Marshall Heilman <Marshall.Heilman@mandiant.com>
Sent: Monday, November 26, 2012 9:17 AM
To: Thad Westbrook
Cc: Pitts, Ted; Jon Neiditz; Rush Smith; Butch.Bowers@wcsr.com; TClaypoole@wcsr.com
Subject: RE: SC Senate Hearing

Hi Thad,
I'll make myself available.

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

From: Thad Westbrook [mailto:thad.westbrook@nelsonmullins.com]
Sent: Monday, November 26, 2012 9:09 AM
To: Marshall Heilman
Cc: Pitts, Ted; Jon Neiditz; Rush Smith; Butch.Bowers@wcsr.com; TClaypoole@wcsr.com
Subject: SC Senate Hearing

Marshall,

The SC Senate has a study committee that is investigating the data breach at the SC Department of Revenue. Ted Pitts informed us a few minutes ago that the committee would like for you to appear on Wednesday and testify during the hearing. Therefore, Ted Pitts will call you to discuss the committee's request and your schedule.

Let us know if you have any questions.

Thank you,
Thad

Nelson Mullins

Thad H. Westbrook
Partner
thad.westbrook@nelsonmullins.com

Nelson Mullins Riley & Scarborough LLP

Meridian, 17th Floor
1320 Main Street, Columbia, SC 29201
Tel: 803.255.5568 Fax: 803.255.9088

www.nelsonmullins.com
(View Bio)

Pitts, Ted

From: Schimsa, Rebecca
Sent: Monday, November 26, 2012 11:56 AM
To: Stirling, Bryan; Pitts, Ted
Subject: FW: Urgent Message from Governor Haley

FYI – SCASA sent an email to over 3,300 of its members (school administrators) this week.

From: Beth Phibbs [mailto:Beth@scasa.org]
Sent: Monday, November 26, 2012 11:54 AM
To: Schimsa, Rebecca
Subject: FW: Urgent Message from Governor Haley

Rebecca,

I am forwarding a copy of the email that went out from our executive director this morning. It went to over 3300 of our members and as you can see, we asked them to forward to their staff and other individuals. Let us know if we can help in any other way.

Thanks,
Beth Phibbs

From: Molly Spearman [mailto:molly@scasa.org]
Sent: Monday, November 26, 2012 11:41 AM
To: Beth Phibbs
Subject: Urgent Message from Governor Haley

Governor Nikki Haley's staff contacted SCASA and ask that we send this urgent message regarding the identity theft at the South Carolina Department of Revenue. Please read and forward the information to your staff and anyone else you think may have been affected by this crime. It is imperative that we take the prescribed precautions. You may go to www.scasa.org or click on the following link -

<http://www.scasa.org/displaycommon.cfm?an=1&subarticlenbr=381>

Over 4.6 million citizens have been affected by this criminal act; however, only 800,000 have registered for credit protection offered free by the state. Please encourage your colleagues, friends, and family to take advantage of this service. Thanks.

Molly Spearman

Pitts, Ted

From: Schimsa, Rebecca
Sent: Wednesday, November 28, 2012 5:52 PM
To: Stirling, Bryan; Godfrey, Rob; Pitts, Ted
Subject: FW: Courtesy Copy: DOD Notifies Troops of South Carolina Cyber Intrusions

FYI re. DOD.

-----Original Message-----

From: Hahn, Lindsey DMA-Fort Meade [mailto:Lindsey.Hahn@dma.mil]
Sent: Wednesday, November 28, 2012 4:20 PM
To: Schimsa, Rebecca
Subject: Courtesy Copy: DOD Notifies Troops of South Carolina Cyber Intrusions

Rebecca,

For your awareness, American Forces Press Service (our print section) released this initial story this afternoon based on your press release. They will do another story once we conduct the interview.

Thanks!
Lindsey

Lindsey A. Hahn
Integrated Plans
Defense Media Activity
(w) 703-692-9703

This bulletin was sent to the following groups of people:

Subscribers of American Forces News Articles (26038 recipients)

You are subscribed to American Forces News Articles for U.S. Department of Defense. This information has recently been updated, and is now available.

DOD Notifies Troops of South Carolina Cyber Intrusions <<http://www.defense.gov/news/newsarticle.aspx?id=118646>>
11/28/2012 02:03 PM CST

DOD Notifies Troops of South Carolina Cyber Intrusions

By Nick Simeone
American Forces Press Service

WASHINGTON, Nov. 28, 2012 - The Defense Department and South Carolina officials are notifying military members and families who paid state income taxes there that they may have been victims of information/identity theft as a result of several recent cyber intrusions.

South Carolina's Department of Revenue reported nearly four million Social Security numbers and several hundred thousand credit and debit card numbers belonging to current and former taxpayers may have been stolen during cyber intrusions in August and September.

While the vast majority of the personal data is believed to have been protected by encryption, state revenue officials said about 16,000 accounts were not, and that anyone who filed a South Carolina income tax return as far back as 1998 could be affected.

The intrusions were discovered last month, officials said. While South Carolina officials believe their system is now secure, Gov. Nikki Haley said the state is offering one year of free credit monitoring and identity protection to anyone who might have been exposed and applies for it. "The number of records breached requires an unprecedented, large-scale response," she said.

In addition to Social Security numbers and credit card information, defense officials said information usually found on the front of checks may also have been exposed.

DOD personnel and their family members who are current or former South Carolina taxpayers, especially those who are living abroad, are urged to visit www.ProtectMyId.com/SCDOR or contact Experian's national consumer assistance center at 1-866-578-5422 by January 31, 2013, to enroll in identity theft protection.

In addition, current and former South Carolina business owners may also contact Dun & Bradstreet Credibility Corp., officials said. Visit www.DandB.com/SC to initiate the registration process or call 1-800-279-9881.

An investigation into the source of the cyber intrusion continues.

Related Sites:

Experian's ProtectMyID <<http://www.defense.gov/news/www.ProtectMyId.com/SCDOR>>

Dun & Bradstreet Credibility Corp. <<http://www.defense.gov/news/www.DandB.com/SC>>

Bookmark and Share <<http://content.govdelivery.com/bulletins/gd/USDOD-5f3259?reqfrom=share>>

Defense Department News Through Facebook On American Forces Press Service's Facebook page, you can post comments and share news, photos and videos. Go to <http://www.facebook.com/pages/American-Forces-Press-Service/65137437532> <<http://www.facebook.com/pages/American-Forces-Press-Service/65137437532>> or search for American Forces Press Service at Facebook.com.

Update your subscriptions, modify your password or e-mail address, or stop subscriptions at any time by clicking on your 'User Profile' page at <https://public.govdelivery.com/accounts/USDOD/subscriber/edit?preferences=true#tab1>. You will need to use your e-mail address to log in. If you have questions or problems with the subscription service, please e-mail support@govdelivery.com.

Have another inquiry? Visit the online FAQ at <http://www.defense.gov/landing/questions.aspx> for up-to-date information.

Get the help you, your family, and fellow servicemembers need, when you need it. Visit www.WarriorCare.mil <<http://www.warriorcare.mil/>> to learn more.

Check out the National Resource Directory at www.nationalresourcedirectory.org <<http://www.nationalresourcedirectory.org/>>, a new web-based resource for wounded, ill and injured service members, veterans, their families, families of the fallen and those who support them from the Departments of Defense, Labor, and Veterans Affairs.

This service is provided to you at no charge by U.S. Department of Defense. Visit us on the web at <http://www.defense.gov/>.

Pitts, Ted

From: Patel, Swati
Sent: Tuesday, December 18, 2012 6:12 PM
To: Pitts, Ted
Subject: Letters
Attachments: Notification letters - vendor selection process.docx; Notifications to Affected Taxpayers
- Background 1.docx

Swati S. Patel
Chief Legal Counsel
Office of the Governor.South Carolina
1205 Pendleton Street
Columbia, SC 29201
DD 803.734.5095

Pitts, Ted

From: Martha Roof <Roof.Martha@doc.sc.gov>
Sent: Thursday, November 08, 2012 1:02 PM
To: Thad.westbrook@nelsonmullins.com
Cc: Pitts, Ted; Baker, Josh; Trevis Shealy
Subject: FW: Inmate access to Protect MY ID.

Thad, I know you have talked to Trevis Shealy in our IT Department about some concerns we have with the 22,000 plus inmates incarcerated at the Department of Corrections and their access to a telephone in order to register with Experian's ProtectMYID Alert.

We have discussed the telephone option with our Operations Staff and while we can provide phone access to each inmate we are concerned that with the wait times and the number of inmates that may decide to register there may not be enough time to have the inmates register prior to January 31, 2013. There is the added difficulty in scheduling inmates for phone access multiple times during the day to get through to Experian. We have to schedule each inmates calls and access to the telephones is restricted. If they cannot get through and have to come back to the phone time and again we will not be able to meet the January 31 time table.

A better option to us would be a **mail-in option** for us to use for our inmates instead of the phone option. Computer access is not an option for inmates and the **mail-in option** would work so much better for us. We would come up with a form for them to complete and have them mail it to Experian with the required information.

A second question for us was could we furnish the Department of Revenue a list of our inmates and have them tell us if the information for the inmate has been compromised? If this could be done we could possibly reduce the number of inmates that would need to register.

Please contact me at 896-1743 or by email so that we can proceed in allowing our inmates access to the protection being offered by the State.

Thanks for your assistance in this matter.

Martha L. Roof, CPA
Deputy Director for Administration
South Carolina Department of Corrections

Pitts, Ted

From: Leon Stavrinakis <lstavrinakis@msn.com>
Sent: Friday, October 26, 2012 4:53 PM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine
Subject: Re: From the Governor's Office re. cyber-attack at DOR

How much is this costing state taxpayers ?

Representative Leon Stavrinakis
Stavrinakis Law Firm
843-813-2800
leon@stavlaw.net
leonstav@schouse.gov

On Oct 26, 2012, at 4:44 PM, "Schimsa, Rebecca" <RebeccaSchimsa@gov.sc.gov> wrote:

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

In regards to the cyber-attack at the Department of Revenue announced this afternoon, we are sending you the following information: (1) the media release from our office (below); (2) the media release from the Department of Revenue (attached); (3) a link to the video of today's press conference; and (4) an invitation to a conference call on Monday morning with Chief Keel, Director Etter, and Inspector General Maley (below).

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

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.

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 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."

-###-

VIDEO OF TODAY'S PRESS CONFERENCE:

The S.C. Department of Revenue announced on October 26, 2012 that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack.

Governor Nikki Haley, South Carolina Law Enforcement Division Chief Mark Keel, United States Secret Service Special Agent in Charge Michael Williams, South Carolina Department of Revenue Director Jim Etter and State Inspector General Patrick Maley today responded to news of the cyber attack with consumer safety solutions during an afternoon press conference.

Video of the press conference is available here: <http://www.youtube.com/watch?v=0Dax66JEzVs&>
Attached you will find a press kit that includes consumer safety solutions.

Anyone who has filed a South Carolina tax return since 1998 should take the following steps:

1. Call 1-866-578-5422 where you will 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.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit <http://www.protectmyid.com/scdor>. For the US Mail service, you will receive notifications via the US mail.

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.

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

Our office has arranged a conference call for members of the General Assembly to be held on Monday, October 29th at 10:00 a.m. with Chief Mark Keel, Director Jim Etter, and Inspector General Pat Maley. The purpose of the conference call is to give you the opportunity to receive information and ask questions about the cyber-attack at the Department of Revenue. There is a limited number of lines available. This call is only intended for you, members of the General Assembly, or a staff member calling in on your behalf.

Call Number: 1-800-670-1742 (No access code is needed.)

Directions:

1. Upon dialing the conference number, each participant will be asked his or her name and then be placed into the conference call.
2. Participants should plan to join the call 5-10 minutes prior to the start of the call.
3. Once the speakers have completed their statements, the call operator will provide instructions for the question and answer portion of the call.
4. All participants will be given the opportunity to ask questions.
5. Questions will be announced in the order that they are received.
6. For operator assistance at any time during the call, please press *0.

-###-

<Media Release from DOR 10.26.2012.pdf>