

From Greg Young, re: numbers for Call Center and ExtendCare info

Greg Young [Greg.Young@experianinteractive.com]

Sent: Tuesday, October 30, 2012 12:47 AM**To:** Stirling, Bryan; Godfrey, Rob**Cc:** Michael Bruemmer [Michael.Bruemmer@experianinteractive.com]; Ozzie Fonseca [ofonseca@experianinteractive.com]

Gentlemen,

Here is information related to the campaign and message points on ExtendCARE (as of 9 pm Pacific). Seeing images of the storms and hope all is well out there.

- Total calls made to the toll free number: 533,000
- Average wait for representative: 9.5 minutes
- Average time representative spends on phone getting information, explaining process and registering individuals: 9 minutes
- Total number of PMID registrations: 287,000

ExtendCARE

This benefit extends our Fraud Resolution Assistance to SC taxpayers after their memberships have expired. By acting quickly and drawing on proven experience in fraud protection Experian Fraud Resolution Experts help you minimize the loss of time and money associated with identity theft.

Experian Fraud Resolution Agents specialize in:

- Working directly with SC taxpayers from beginning to end to help resolve identity theft once their membership begins and long after it expires.
- Placing a temporary 90-day or extended seven-year fraud alert on consumers' Experian credit reports, as requested, to help stop fraudulent new accounts from opening.
- Sharing the fraud alert with the Equifax® and TransUnion® credit bureaus.
- Assisting with the dispute process for inaccurate information or fraudulent activity on Experian credit reports.
- Drafting and providing dispute letters for SC taxpayers to report credit fraud to Equifax and TransUnion.
- Assisting in scheduling conference calls with financial providers, creditors and service providers to dispute fraudulent charges and accounts.
- Interacting with law enforcement or government agencies to work toward a resolution and assist with filing a police report, if possible.
- Providing copies of all necessary letters to report credit fraud and identity theft to creditors, credit reporting agencies or others who may be involved in the process of reclaiming SC taxpayers' identities.
- Reviewing credit records to help SC taxpayers determine potential areas of fraud.

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 Greg Young, re: URGENT

Greg Young [Greg.Young@experianinteractive.com]

Sent: Monday, October 29, 2012 5:34 PM

To: Stirling, Bryan; Godfrey, Rob

Cc: Michael Bruemmer [Michael.Bruemmer@experianinteractive.com]; Ozzie Fonseca [ofonseca@experianinteractive.com]

Gentlemen,

Can you get word out that people should NOT put middle initials in the first name field (see below). For some reason it's creating an issue that is slowing down the registration process for folks. Again, if the media can communicate that people registering for PMID should Not use a middle initial. Let me know if you have questions. We want to create speed in all facets of the process and deliver a great experience.

Best,

GY

You are only 3 steps away from obtaining powerful identity protection.



First Name

Last Name

Suffix

Address

Zip Code

City

State

Email

Have you lived at your current address for more than 6 months? ☒ Yes ☐ No

☐ Yes, please send me important identity theft information and special offers from Experian

Submit & Continue



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 Greg Young, re: FS overview

Greg Young [Greg.Young@experianinteractive.com]

Sent: Monday, October 29, 2012 3:44 PM**To:** Stirling, Bryan; Godfrey, Rob**Cc:** Michael Bruemmer [Michael.Bruemmer@experianinteractive.com]; Ozzie Fonseca [ofonseca@experianinteractive.com]

Gentlemen –

Here is a summation of FS:

Process:

- Those individuals that already enrolled in ProtectMyID™ will get an email alerting them to the availability of Family Secure and how to register their minors who were listed on tax paperwork as dependents.
- Those that have not registered yet with the ProtectMyID product will be sent an email with Family Secure registration directions upon completing the ProtectMyID registration.

Requirement:

- Individuals must sign up for ProtectMyID first. Once they are registered, notification and a registration code (different from the one used for ProtectMyID) will be sent to them, with directions what to do to register with Family SecureSM. If they do not have minors listed as dependents, then they can ignore the notice. As with ProtectMyID, the Family Secure registration process may be completed via the phone with a live representative. For the Family Secure product, an email address is required.

Your other questions:

- Parents register their children as part of Family Secure.
- The primary benefit that Family Secure brings to bear in this situation is that it monitors the identity (primarily the SSN) of the minor who has no credit report – thus no alerts. Once registered, in the event a child does have a credit file, if any credit, loan or similar account is opened with that information, the parents are alerted to call customer care. (Detail of the alert on minors is not released unless or until the Parent authenticates themselves with customer care as the parent or guardian of the minor.)

Family Secure features:Coverage:

- One adult
- Any amount of minors (5 are allowed to enroll on the website; for more than 5, the customer must call Customer Care)

Key Benefits the adult receives:

- \$2 million product Guarantee covers the whole family
- Score Tracker
- Fraud Resolution

Benefits the minors receive:

- **Monthly monitoring for existence of minor's credit report**
 - If a credit report is found, then we monitor for any changes to that report

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

Updated Message for 2100

Haltiwanger, Katherine

Sent: Monday, October 29, 2012 1:23 PM
To: Smoak, Carol
Cc: Godfrey, Rob; Jones, Sheila; Stirling, Bryan
Importance: High

Carol, please have 2100 changed today by 5 p.m. to the following message:

You have reached the Office of Governor Nikki Haley. The office is open Monday through Friday, 8:30 a.m. to 5:00 p.m. If you are calling about the cyber attack, you can visit www.protectmyid.com/scdor and enter the code SCDOR123. Sign-up ends on January 31, 2013. If you do not have access to the internet, you can call 1-866-578-5422 (say the # twice). Thank you.

Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

Godfrey, Rob

Sent: Monday, October 29, 2012 1:22 PM

Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

COLUMBIA, S.C. – Governor Nikki Haley, South Carolina Law Enforcement Division Chief Mark Keel and South Carolina Department of Revenue (DOR) Director Jim Etter today provided reporters with an update on the S.C. DOR information security breach and discussed consumer safety solutions available to South Carolinians during a Statehouse press conference. S.C. DOR announced on October 26, 2012 that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers had been exposed in a cyber attack.

Video of today's Statehouse press conference, including remarks by the governor and Chief Keel as well as a media availability, is available here: <http://www.youtube.com/watch?v=ni9jQS3Nb80>

As of Monday morning, the Experian call center set up to assist South Carolina taxpayers had received approximately 455,000 calls and approximately 154,000 signups. Gov. Haley and Chief Keel reiterated that anyone who has filed a South Carolina tax return since 1998 should take the following steps:

- 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.)
- For any South Carolina taxpayer residing in South Carolina 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. Every South Carolina taxpayer who takes the time to sign up will be afforded the protection, and that protection is retroactive. South Carolina taxpayers have until the end of January, 2013 to sign up. South Carolina taxpayers who sign up for protection will be notified about how to sign up for a "Family Secure Plan" if they claim minors as dependents.

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

Fw: A question

Veldran, Katherine

Sent: Monday, October 29, 2012 11:30 AM**To:** Stirling, Bryan; Pitts, Ted; Schimsa, Rebecca

From: Rep. Phyllis Henderson [mailto:██████████@gmail.com]**Sent:** Sunday, October 28, 2012 07:10 PM**To:** Veldran, Katherine**Subject:** A question

Katherine:

First, I want to make sure I have your correct phone #. I called 803-767-7583 and got a generic voicemail so wanted to make sure that was right.

Second, I have received several calls and emails about the computer hacking situation - as I'm sure most of my colleagues and you have, too. One of the biggest complaints is that the media reports made it sound like an individual could call the 866 number and find out if they are affected or not. All you are told is the activation code for protectmyid.com and then are told that IF you were not affected you will have to pay for your membership!

People want to know if they were affected or not and I think we owe them that information. What is the plan? I hope we will find out more tomorrow morning during the conference call. Phyllis

--

Representative Phyllis Henderson
SC House District 21
864-423-3149

Sign up for my DIstrict 21 newsletter! Click here:

<http://oi.vresp.com?fid=58d852d7a6>

On Twitter: @phyllish21

View my vote record: <http://is.gd/henderson21> and click on "voting record"

Updated Information

Haltiwanger, Katherine

Sent: Monday, October 29, 2012 9:48 AM

To: Jones, Sheila; Thomas, Katherine

Cc: Glover, Christine; Baker, Josh; Bondurant, Kate; Stirling, Bryan; Godfrey, Rob; Hall, Taylor; Jones, Sheila; LeMoine, Leigh; Patel, Swati; Peters, Hal; Pitts, Ted; Schimsa, Rebecca; Soura, Christian; Taillon, Jeff; Veldran, Katherine; Walker, Madison; Walls, Courtney

Importance: High

UPDATED INSTRUCTIONS FOR CONSITUENTS:

As of this morning, the steps to receive Protect My ID have changed. Please notify constituents that they can go on www.protectmyid.com/scdor and enter the code SCDOR123 (not case sensitive). Sign-up ends on January 31. If they don't have access to the internet, they can call 1-866-578-5422.

Please let me know if you have any questions.

Thanks,

Katherine

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

Veldran, Katherine

Sent: Monday, October 29, 2012 9:04 AM

To: Stirling, Bryan

From: Taillon, Jeff

Sent: Monday, October 29, 2012 08:52 AM

To: Pitts, Ted; Veldran, Katherine

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

Jeff Taillon

(803) 734-5129|Direct Line

(803) 767-7653|Cell

From: Rita Allison [mailto:██████████@charter.net]

Sent: Monday, October 29, 2012 8:49 AM

To: Taillon, Jeff

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

My people are most concerned about giving ss# to a private company. Thoughts? Rita
Sent from my Verizon Wireless 4G LTE DROID

"Taillon, Jeff" <JeffTaillon@gov.sc.gov> wrote:

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

State officials will provide update on S.C. DOR information security breach

COLUMBIA, S.C. – Governor Nikki Haley, South Carolina Law Enforcement Division (SLED) Chief Mark Keel, South Carolina Department of Revenue (DOR) Director Jim Etter and other officials will hold a press conference TODAY, Monday, October 29, at 10:00 AM to update the people of South Carolina on the DOR information security breach and reiterate what every South Carolinian can and should do to protect themselves. The press conference will be held in the first floor lobby of the Statehouse.

WHO: Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter and other officials

WHAT: DOR information security breach update

WHEN: TODAY, Monday, October 29, 10:00 AM

WHERE: S.C. Statehouse, first floor lobby, Columbia S.C.

-###-

Jeff Taillon

(803) 734-5129|Direct Line

(803) 767-7653|Cell

Re: Conference Call

Jeff Gossett [JeffGossett@scsenate.gov]

Sent: Sunday, October 28, 2012 9:58 PM**To:** Stirling, Bryan

I understand you and Mike talked about the conference call. If you end up sending something new to all Senators, please include Mike and I on the message.

Thanks,

Jeff

His email, if you don't have it, is MikeHitchcock@scsenate.gov

On Oct 26, 2012, at 10:09 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

Can I call you tomorrow on this? Been a very busy day.

From: Jeff Gossett [mailto:JeffGossett@scsenate.gov]

Sent: Friday, October 26, 2012 10:07 PM

To: Stirling, Bryan

Subject: Conference Call

I know it's probably been a bad day, but did y'all really send this out as a press release?

If you want info to go to legislators, you can get it to Charles and I and we can get it to them for you.

Jeff

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.

-###-

Fw: Fwd: Website email from Lisa Hoffman

Veldran, Katherine

Sent: Sunday, October 28, 2012 2:43 PM

To: Stirling, Bryan; Pitts, Ted; Godfrey, Rob

Cc: Schimsa, Rebecca

From: Garry R. Smith [mailto:GarrySmith@schouse.gov]

Sent: Saturday, October 27, 2012 07:13 PM

To: Veldran, Katherine

Subject: Fwd: Website email from Lisa Hoffman

Katherine, the questing from this constituent is what do they do if they do not have Internet access. Can you help with this?

Thanks!

Sent from my iPad

Begin forwarded message:

From: "[REDACTED]@aol.com" <[REDACTED]@aol.com>

Date: October 27, 2012, 4:52:56 PM EDT

Subject: Website email from Lisa Hoffman

What do people who do not have internet access do about the SCDOR security breach?

Thanks!

Lisa [REDACTED]

[REDACTED]
simpsonville, SC [REDACTED]

Fw: Problems re Social Security Number Theft -- Senator Rose

Veldran, Katherine

Sent: Sunday, October 28, 2012 2:43 PM**To:** Stirling, Bryan; Pitts, Ted; Godfrey, Rob**Cc:** Schimsa, Rebecca

From: Michael Rose [mailto:[REDACTED]@sc.rr.com]**Sent:** Saturday, October 27, 2012 11:18 PM**To:** Veldran, Katherine**Cc:** [REDACTED]@sc.rr.com <[REDACTED]@sc.rr.com>; 'Vivian Rose' <[REDACTED]@sc.rr.com>**Subject:** Problems re Social Security Number Theft -- Senator Rose

Katherine,

The Governor may want to know the following complaints about the remedies offered the public regarding the theft of social security numbers, etc.:

1. A prominent Republican has complained to me that it was impossible for him to get anyone to answer at the toll free number to which the public has been encouraged to call; and
2. Another citizen has complained that she cannot find where to log in as instructed. See below.

Thank you.

Mike Rose

From: Bonnie [REDACTED] [mailto:[REDACTED]@bellsouth.net]**Sent:** Saturday, October 27, 2012 1:38 PM**To:** vivian rose**Subject:**

Hey, Vivian. I guess you are as upset as millions of us about the social security #'s, credit card and debit card #'s being compromised. It is so hard to understand why our state did not have a better system of protection. Too hard to believe.

However, I used the number in the paper to call; and, I got the password for SCDOR123, but when I go on the computer to log in--I can't find where to do it. Can you offer me any suggestions? Sorry to bother you. This morning, my facebook was hacked, but my security blocked it. It told me that a computer or mobile device in Cummings, GA tried to get into my facebook. It could not have happened at a worse time; and, I pray it had nothing to do with the other problem.

Family Secure

Ozzie Fonseca [ofonseca@experianinteractive.com]

Sent: Sunday, October 28, 2012 2:14 PM

To: Stirling, Bryan; Jim Etter (etter_jf@sctax.org)

Gentlemen:

I spoke with Greg Young and he asked me to set up a call with you to further discuss Family Secure. I'm available at your convenience.

Please let me know when you will have a moment and I will send a meeting invitation.

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

Blog: www.Experian.com/blogs/data-breach
Follow us on Twitter: 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.

FW: SC tax record hack

Greg Young [Greg.Young@experianinteractive.com]

Sent: Sunday, October 28, 2012 1:09 PM**To:** Stirling, Bryan; Godfrey, Rob

Gentlemen,

Have we thought about providing this confirmation and what that communication will look like (below) or are we foregoing this since we are basically offering the protection to everyone that calls in (that has been a taxpayer between 1998 and now)?

I know we are in the midst of securing a solution to the roll out of Family Secure, but do you (we) want to start thinking about how you want to position the child risk messaging now? I can finesse, but let me know positioning/messaging that's critical for you all.

GY

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: Ryan Naquin [mailto:rnaquin@wpde.com]**Sent:** Sunday, October 28, 2012 10:00 AM**To:** Greg Young**Subject:** SC tax record hack

Hey Greg,

I have talked with the SC DOR and know that Experian has no way of knowing at this time who has been affected in the South Carolina tax information hack. I just wanted to know, when you guys do find out and if someone who set up an Experian account, how will you notify them? Will it be an email? Will it be a big ALERT on the page when you log in? if someone takes time to get this done, will an ALERT be on their home screen as soon as they sign up? And with this breach, should parents be concerned about their children's identity as well?

Hope this makes sense.

Thanks,

Ryan Naquin
Reporter
NewsChannel 15 WPDE
Myrtle Beach, SC
843-742-9833

Fw: From the Governor's Office re. cyber-attack at DOR

Schimsa, Rebecca

Sent: Sunday, October 28, 2012 9:14 AM

To: Stirling, Bryan

Cc: Pitts, Ted; Veldran, Katherine

From: James Smith [mailto:JamesSmith@schouse.gov]

Sent: Sunday, October 28, 2012 05:59 AM

To: Schimsa, Rebecca

Cc: Pitts, Ted; Veldran, Katherine; Mark Keel <mkeel@sled.sc.gov>; Kirkland T. Smith <Kirkland@KirklandSmith.com>; Rep. James E. Smith Jr. <James@JamesSmith.com>

Subject: Re: From the Governor's Office re. cyber-attack at DOR

What about the SSN's of SC Children? If you have dependents listed on your return each have a name, date of birth and SSN provided. Is that information at risk and I don't believe they can access Protect My ID .com as a minor? How can the people of SC protect the ID's of their children? Are we certain that the risk is limited to only those that "filed" a tax return?

Thanks, James

On Oct 26, 2012, at 4:46 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>

FW: From Greg Young, re: Answers to questions - round 2

Greg Young [Greg.Young@experianinteractive.com]

Sent: Saturday, October 27, 2012 9:44 PM**To:** Godfrey, Rob**Cc:** Stirling, Bryan; [REDACTED]@gmail.com; [REDACTED]@gmail.com)

Rob,

Should the reporter respond as she has been and indicate that's not enough, you may want to reference these points from your release. The risk of not immediately registering – i.e., the exposure period without the protection of PMID – is something Bryan and Tim suggested should come from the State. I presume this would be a ranking technology official.

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.

In addition, individuals with online access to their credit card/bank card statements have daily access to the transactions and balances. Most can have alerts set up. Credit monitoring does not send immediate usage alerts like credit card services do. Credit monitoring provides alerts for things like if a new credit card is opened in the individuals name or if there is a "hard inquiry" that is usually initiated when one applies for some type of loan. These are timely, but not immediate, like the alerts provided by credit cards themselves.

Let me know if you have more questions on this – I strongly recommend you run this by a ranking member in the technology office to get input on these points as they relate to the question. I think crafting that FAQ and posting to a State blog or media page is sounding more and more like a good idea.

Finally, despite her disappointment at what was provided as answers, she has known since we first talked that I would not be able to answer all the questions. She also did not offer any preference in the order they were answered. Instead, she responded to our efforts in the negative. It's unfortunate since our delay has nothing to do about stalling and is a result of our focus on accuracy.

We'll talk in the morning.

GY

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: Courrege, Diette [mailto:dcourrege@postandcourier.com]
Sent: Saturday, October 27, 2012 6:27 PM
To: Greg Young
Cc: Godfrey, Rob (RobGodfrey@gov.sc.gov)
Subject: RE: From Greg Young, re: Answers to questions - round 2

Rob, my question was this:

Jim Etter with the state Department of Revenue said it didn't matter if someone signed up today or in a month for the Experian service; they wouldn't be hurt by waiting. Is that true? If so, can you explain why? It didn't make sense to me. Isn't the idea of credit monitoring that you would know asap if someone were using your identity to make atypical purchases, so it would be best to have that now vs. to wait a few weeks when someone could've used your identity to buy those plasma TVs? When I asked Jim, he said that was a good point and that would be a question for Experian. I do know a lot of people are concerned that they're not able to access the system now

From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Saturday, October 27, 2012 9:25 PM
To: Courrege, Diette
Cc: Godfrey, Rob (RobGodfrey@gov.sc.gov)
Subject: RE: From Greg Young, re: Answers to questions - round 2

I believe that contact should be Rob Godfrey (cc'd here). It is my understanding that he can identify an individual to respond, or can get the information from a qualified expert. I will continue to provide you answers to questions related to the monitoring and ID protection product.

Best,

Greg

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: Courrege, Diette [<mailto:dcourrege@postandcourier.com>]
Sent: Saturday, October 27, 2012 6:22 PM
To: Greg Young
Subject: RE: From Greg Young, re: Answers to questions - round 2

The state being who? Etter didn't have the information to answer the question.

From: Greg Young [<mailto:Greg.Young@experianinteractive.com>]
Sent: Saturday, October 27, 2012 9:21 PM
To: Courrege, Diette
Subject: FW: From Greg Young, re: Answers to questions - round 2

Diette –

In regards to Mr. Etter's comments, I have confirmed that the State would prefer to answer that question. Again, I am working as quickly as I can get confirmation on the accuracy of the information I am providing.

Best,

Greg

Greg Young
Director, Public Relations
Experian Consumer Services

From: Greg Young
Sent: Saturday, October 27, 2012 6:15 PM
To: 'Courrege, Diette'
Subject: RE: From Greg Young, re: Answers to questions - round 2

Hi Diette –

Responses below. I apologize for the delay, but I am committed to getting you accurate information.

Greg Young
Director, Public Relations
Experian Consumer Services

From: Courrege, Diette [<mailto:dcourrege@postandcourier.com>]
Sent: Saturday, October 27, 2012 5:56 PM
To: Greg Young
Subject: RE: From Greg Young, re: Answers to questions - round 1

This is really disappointing, Greg. Why did you reduce my questions to those three? I'm most interested in

answers that aren't listed here, specifically:

- How many folks have signed up for the credit protection thus far? **WE ARE STILL DETERMINING THAT NUMBER**
- How much will the service cost the state on a per person basis? (I know the contract was signed yesterday and the total dollar figure depends on how many folks sign up). **THE STATE WILL NEED TO ANSWER THAT QUESTION**
- Jim Etter with the state Department of Revenue said it didn't matter if someone signed up today or in a month for the Experian service; they wouldn't be hurt by waiting. Is that true? If so, can you explain why? It didn't make sense to me. Isn't the idea of credit monitoring that you would know asap if someone were using your identity to make atypical purchases, so it would be best to have that now vs. to wait a few weeks when someone could've used your identity to buy those plasma TVs? When I asked Jim, he said he didn't know and that was a question for y'all. I do know a lot of people are concerned that they're not able to access the system now. **I AM WORKING ON GETTING YOU A CLEAR ANSWER ON THIS.**
- 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? **SOUTH CAROLINA 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 AFFECTED TAXPAYER. SOUTH CAROLINA WILL KEEP MONITORING THE CALL CENTER AND UNTIL THE STATE IS SURE ALL AFFECTED TAXPAYERS ARE ABLE TO REGISTER WITHOUT UNREASONABLE DELAY WE WILL MAINTAIN THE CURRENT PROCESS. THE CODE BEING DISTRIBUTED NOW IS A "ONE-TIME" USE. ANYONE WHO HAS USED THE CURRENT CODE WILL NOT BE REQUIRED TO CALL BACK IN FOR AN INDIVIDUAL CODE. THEIR REGISTRATIONS ARE COMPLETED.**
- I'm told you provide this service for a year for free. What happens at the end of the year? Are you automatically re-enrolled for a fee, or will the company notify SC residents that their time is up and to continue the service costs \$XXX. **RE-ENROLLMENT WILL BE OFFERED TO EACH INDIVIDUAL AT THE END OF A YEAR.**

From: Greg Young [<mailto:Greg.Young@experianinteractive.com>]

Sent: Saturday, October 27, 2012 8:52 PM

To: Courrege, Diette

Subject: From Greg Young, re: Answers to questions - round 1

Diette,

Here are three answers. Struggling on 4th. Will get that to you in next 10 minutes.

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. **ALL SC TAXPAYERS FROM 1998 TO PRESENT WILL BE COVERED BY THIS SERVICE AT NO COST TO THEM.**
2. 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.**
3. 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

FW: From Greg Young, re: Answers to questions - round 2

Greg Young [Greg.Young@experianinteractive.com]

Sent: Saturday, October 27, 2012 9:27 PM

To: Godfrey, Rob; Stirling, Bryan; [REDACTED]@gmail.com' [REDACTED]@gmail.com)

Gentlemen,

My second email to the reporter.

GY

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: Greg Young

Sent: Saturday, October 27, 2012 6:15 PM

To: 'Courrege, Diette'

Subject: RE: From Greg Young, re: Answers to questions - round 2

Hi Diette –

Responses below. I apologize for the delay, but I am committed to getting you accurate information.

Greg Young

Director, Public Relations

Experian Consumer Services

From: Courrege, Diette [<mailto:dcourrege@postandcourier.com>]

Sent: Saturday, October 27, 2012 5:56 PM

To: Greg Young

Subject: RE: From Greg Young, re: Answers to questions - round 1

This is really disappointing, Greg. Why did you reduce my questions to those three? I'm most interested in answers that aren't listed here, specifically:

- How many folks have signed up for the credit protection thus far? **WE ARE STILL**

DETERMINING THAT NUMBER

- How much will the service cost the state on a per person basis? (I know the contract was signed yesterday and the total dollar figure depends on how many folks sign up). **THE STATE WILL NEED TO ANSWER THAT QUESTION**
- Jim Etter with the state Department of Revenue said it didn't matter if someone signed up today or in a month for the Experian service; they wouldn't be hurt by waiting. Is that true? If so, can you explain why? It didn't make sense to me. Isn't the idea of credit monitoring that you would know asap if someone were using your identity to make atypical purchases, so it would be best to have that now vs. to wait a few weeks when someone could've used your identity to buy those plasma TVs? When I asked Jim, he said he didn't know and that was a question for y'all. I do know a lot of people are concerned that they're not able to access the system now. **I AM WORKING ON GETTING YOU A CLEAR ANSWER ON THIS.**
- 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? **SOUTH CAROLINA 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 AFFECTED TAXPAYER. SOUTH CAROLINA WILL KEEP MONITORING THE CALL CENTER AND UNTIL THE STATE IS SURE ALL AFFECTED TAXPAYERS ARE ABLE TO REGISTER WITHOUT UNREASONABLE DELAY WE WILL MAINTAIN THE CURRENT PROCESS. THE CODE BEING DISTRIBUTED NOW IS A "ONE-TIME" USE. ANYONE WHO HAS USED THE CURRENT CODE WILL NOT BE REQUIRED TO CALL BACK IN FOR AN INDIVIDUAL CODE. THEIR REGISTRATIONS ARE COMPLETED.**
- I'm told you provide this service for a year for free. What happens at the end of the year? Are you automatically re-enrolled for a fee, or will the company notify SC residents that their time is up and to continue the service costs \$XXX. **RE-ENROLLMENT WILL BE OFFERED TO EACH INDIVIDUAL AT THE END OF A YEAR.**

From: Greg Young [<mailto:Greg.Young@experianinteractive.com>]

Sent: Saturday, October 27, 2012 8:52 PM

To: Courrege, Diette

Subject: From Greg Young, re: Answers to questions - round 1

Diette,

Here are three answers. Struggling on 4th. Will get that to you in next 10 minutes.

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. **ALL SC TAXPAYERS FROM 1998 TO PRESENT WILL BE COVERED BY THIS SERVICE AT NO COST TO THEM.**

2. 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.**
3. 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

Re: FINALS FOR POST AND COURIER

Tim Pearson [mailto:[REDACTED]@gmail.com]

Sent: Saturday, October 27, 2012 8:57 PM**To:** Greg Young [Greg.Young@experianinteractive.com]; Godfrey, Rob; Stirling, Bryan

I think that's great.

Thanks, Greg.

Sent from my Verizon Wireless BlackBerry

From: Greg Young <Greg.Young@experianinteractive.com>**Date:** Sun, 28 Oct 2012 00:55:54 +0000**To:** [REDACTED]@gmail.com <[REDACTED]@gmail.com>; Godfrey, Rob (RobGodfrey@gov.sc.gov) <RobGodfrey@gov.sc.gov>; Stirling, Bryan (BryanStirling@gov.sc.gov) <BryanStirling@gov.sc.gov>**Subject:** RE: FINALS FOR POST AND COURIER

1. 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? **SOUTH CAROLINA 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 AFFECTED TAXPAYER. SOUTH CAROLINA WILL KEEP MONITORING THE CALL CENTER AND UNTIL THE STATE IS SURE ALL AFFECTED TAXPAYERS ARE ABLE TO REGISTER WITHOUT UNREASONABLE DELAY WE WILL MAINTAIN THE CURRENT PROCESS. THE CODE BEING DISTRIBUTED NOW IS A "ONE-TIME" USE. ANYONE WHO HAS USED THE CURRENT CODE WILL NOT BE REQUIRED TO CALL BACK IN FOR AN INDIVIDUAL CODE. THEIR REGISTRATIONS ARE COMPLETED.**

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: Tim Pearson [mailto:[REDACTED]@gmail.com]

Sent: Saturday, October 27, 2012 5:48 PM

To: Greg Young; Godfrey, Rob (RobGodfrey@gov.sc.gov); Stirling, Bryan (BryanStirling@gov.sc.gov)

Subject: Re: FINALS FOR POST AND COURIER

What we have doesn't answer their question, or mine. Let's get it right and fire it off in the next 10 minutes.

Sent from my Verizon Wireless BlackBerry

From: Greg Young <Greg.Young@experianinteractive.com>

Date: Sun, 28 Oct 2012 00:46:10 +0000

To: [REDACTED]@gmail.com<[REDACTED]@gmail.com>; Godfrey, Rob (RobGodfrey@gov.sc.gov) <RobGodfrey@gov.sc.gov>; Stirling, Bryan (BryanStirling@gov.sc.gov) <BryanStirling@gov.sc.gov>

Subject: RE: FINALS FOR POST AND COURIER

Latest from PC:

Greg, I know you're trying to do this as fast as you can, but we're running up against deadline. If I don't have it by 9, it's going to start causing some problems for us. Is there any way you can send me whatever you've got? Obviously, some of those questions are far more important for the reader to understand tomorrow.

I think we can go with what we have and I can clarify anything. Otherwise we miss the window, which I know Rob didn't want to do.

GY

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: Tim Pearson [[mailto:\[REDACTED\]@gmail.com](mailto:[REDACTED]@gmail.com)]

Sent: Saturday, October 27, 2012 5:40 PM

To: Greg Young; Godfrey, Rob (RobGodfrey@gov.sc.gov); Stirling, Bryan (BryanStirling@gov.sc.gov)

Subject: Re: FINALS FOR POST AND COURIER

Sorry Greg - not trying to be difficult here, and the answer to 1 is perfect, but not sure 2 answers the question yet. Does entering the code the first time mean that they will never have to enter it again, and we will take care of contacting them if anything is necessary going forward?

Sent from my Verizon Wireless BlackBerry

From: Greg Young <Greg.Young@experianinteractive.com>

Date: Sun, 28 Oct 2012 00:33:58 +0000

To: Godfrey, Rob (RobGodfrey@gov.sc.gov)<RobGodfrey@gov.sc.gov>; Stirling, Bryan (BryanStirling@gov.sc.gov)<BryanStirling@gov.sc.gov>; [REDACTED]@gmail.com' [REDACTED]@gmail.com' [REDACTED]@gmail.com>

Subject: FINALS FOR POST AND COURIER

Gents,

She is definitely ready for this, per her last email. Can I send?

GY

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. **ALL SC TAXPAYERS FROM 1998 TO PRESENT WILL BE COVERED BY THIS SERVICE AT NO COST TO THEM.**
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? **SOUTH CAROLINA 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 AFFECTED TAXPAYER. SOUTH CAROLINA WILL KEEP MONITORING THE CALL CENTER AND UNTIL THE STATE IS SURE ALL AFFECTED TAXPAYERS ARE ABLE TO REGISTER WITHOUT UNREASONABLE DELAY WE WILL MAINTAIN THE CURRENT PROCESS.**
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

RE: FINALS FOR POST AND COURIER

Greg Young [Greg.Young@experianinteractive.com]

Sent: Saturday, October 27, 2012 8:42 PM**To:** [REDACTED]@gmail.com; Godfrey, Rob; Stirling, Bryan

Yes – but I didn't read that as the question. Why don't I submit to her and tell her she can contact me with additional questions related to these four. If that comes up, I can clarify?

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: Tim Pearson [mailto:[REDACTED]@gmail.com]**Sent:** Saturday, October 27, 2012 5:40 PM**To:** Greg Young; Godfrey, Rob (RobGodfrey@gov.sc.gov); Stirling, Bryan (BryanStirling@gov.sc.gov)**Subject:** Re: FINALS FOR POST AND COURIER

Sorry Greg - not trying to be difficult here, and the answer to 1 is perfect, but not sure 2 answers the question yet. Does entering the code the first time mean that they will never have to enter it again, and we will take care of contacting them if anything is necessary going forward?

Sent from my Verizon Wireless BlackBerry

From: Greg Young <Greg.Young@experianinteractive.com>**Date:** Sun, 28 Oct 2012 00:33:58 +0000**To:** Godfrey, Rob (RobGodfrey@gov.sc.gov)<RobGodfrey@gov.sc.gov>; Stirling, Bryan (BryanStirling@gov.sc.gov)<BryanStirling@gov.sc.gov>;

[REDACTED]@gmail.com' ([REDACTED]@gmail.com)<[REDACTED]@gmail.com>

Subject: FINALS FOR POST AND COURIER

Gents,

She is definitely ready for this, per her last email. Can I send?

GY

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. **ALL SC TAXPAYERS FROM 1998 TO PRESENT WILL BE COVERED BY THIS SERVICE AT NO COST TO THEM.**

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? **SOUTH CAROLINA 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 AFFECTED TAXPAYER. SOUTH CAROLINA WILL KEEP MONITORING THE CALL CENTER AND UNTIL THE STATE IS SURE ALL AFFECTED TAXPAYERS ARE ABLE TO REGISTER WITHOUT UNREASONABLE DELAY WE WILL MAINTAIN THE CURRENT PROCESS.**
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

Re: Rob and Bryan, please review - TIME SENSITIVE

Godfrey, Rob

Sent: Saturday, October 27, 2012 8:29 PM

To: Stirling, Bryan; Greg.Young@experianinteractive.com

Cc: Ken.Chaplin@experianinteractive.com; Joshua.Light@experianconsumerdirect.com; Ken.Bixler@experianinteractive.com; ofonseca@experianinteractive.com; [REDACTED]@gmail.com

Looping Tim in here.

From: Stirling, Bryan

Sent: Saturday, October 27, 2012 08:26 PM

To: 'Greg.Young@experianinteractive.com' <Greg.Young@experianinteractive.com>; Godfrey, Rob

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

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

RE: Rob and Bryan, please review - TIME SENSITIVE

Greg Young [Greg.Young@experianinteractive.com]

Sent: Saturday, October 27, 2012 8:20 PM

To: Godfrey, Rob; [REDACTED]@gmail.com; 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]

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 OPTION 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

RE: Rob and Bryan, please review - TIME SENSITIVE

Greg Young [Greg.Young@experianinteractive.com]

Sent: Saturday, October 27, 2012 8:10 PM

To: Godfrey, Rob; Stirling, Bryan

Cc: [REDACTED]@gmail.com

Gentlemen,

Something to think about for our call tomorrow morning:

Is there a blog or State digital publishing property that we could assemble what would amount to an FAQ and get a lot of the basic information out there? Then we could point media there?

GY

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 5:01 PM

To: Greg Young; Stirling, Bryan

Cc: Ken Chaplin; Joshua Light; Ken Bixler; Ozzie Fonseca; [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 OPTION 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

Your message

Ozzie Fonseca [ofonseca@experianinteractive.com]

Sent: Saturday, October 27, 2012 4:20 PM

To: Stirling, Bryan; Greg Young [Greg.Young@experianinteractive.com]

Bryan:

My apologies for not being able to pick up your call. I'm on the phone coordinating other aspects of the initiative.

I spoke with Greg and it might be beneficial to let him be your main point of contact going forward so that you have the most up to date information.

Greg should be able to send you his comments soon.

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-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.

I will call you at 1:30 Eastern

Ozzie Fonseca [ofonseca@experianinteractive.com]

Sent: Saturday, October 27, 2012 12:49 PM

To: Stirling, Bryan

I was going to call you in 10 minutes but I have limited information. I have a meeting with the team in about 20 minutes, and will call you right after. From what I understand the recording approach is paying off.

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.

Re: From the Governor's Office re. cyber-attack at DOR

Schimsa, Rebecca

Sent: Saturday, October 27, 2012 10:54 AM

To: Stirling, Bryan

Will do.

From: Stirling, Bryan

Sent: Friday, October 26, 2012 10:43 PM

To: Schimsa, Rebecca

Subject: Re: From the Governor's Office re. cyber-attack at DOR

Please keep forwarding any legislative responses. I will call them if I have the number if not I will email them.
Thank you.

From: Schimsa, Rebecca

Sent: Friday, October 26, 2012 10:40 PM

To: Stirling, Bryan

Subject: Fw: From the Governor's Office re. cyber-attack at DOR

FYI.

From: Leon Stavrinakis [mailto:[REDACTED]@msn.com]

Sent: Friday, October 26, 2012 10:28 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: [REDACTED]@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:[REDACTED]@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>

Sunday call code

Jim Etter [Etter_JF@sctax.org]

Sent: Saturday, October 27, 2012 8:16 AM

To: Stirling, Bryan

Bryan

I have the code

Thanks

Sent from my iPhone

RE: From Greg Young, re: proposed statement

Greg Young [Greg.Young@experianinteractive.com]

Sent: Friday, October 26, 2012 11:11 PM

To: Godfrey, Rob; Stirling, Bryan

Cc: Ken Chaplin [Ken.Chaplin@experianinteractive.com]

We feel that the statement should come from the State. It would be strange having the company answer for the state in this situation, but we should be included.

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: Friday, October 26, 2012 8:10 PM

To: Greg Young; Stirling, Bryan

Cc: Ken Chaplin

Subject: Re: From Greg Young, re: proposed statement

Is this statement/release coming from Experian?

From: Greg Young [mailto:Greg.Young@experianinteractive.com]

Sent: Friday, October 26, 2012 10:56 PM

To: Stirling, Bryan

Cc: Godfrey, Rob; Ken Chaplin <Ken.Chaplin@experianinteractive.com>

Subject: From Greg Young, re: proposed statement

Statement related to South Carolina citizens' inability to access breach protection services via phone.

The Office of the Governor has worked closely with Experian's ProtectMyID™ to offer taxpayers affected by the recent data breach the opportunity to sign up for one year of credit monitoring and identity protection. The offer has already generated hundreds of thousands of calls. Unfortunately, some residents have experienced challenges getting through due to the high call volume. The Office of the Governor has worked closely with Experian to implement a solution that will help remedy this.

Starting Saturday, October 27 at 11 a.m. Eastern Time, callers will immediately receive a pre-recorded message offering the option to wait for a live operator, or follow instructions to initialize the ProtectMyID product online.

"Despite our preparation, we -- along with our partner, Experian -- were unprepared for the overwhelming response to the breach announcement," said [NAME]. "Unintentionally, an exaggerated sense of urgency was created by omitting to note the registration process will be available for weeks. We deeply regret the inconvenience and anxiety this has caused the citizens of South Carolina and have moved as quickly as possible with Experian to implement a solution."

[please edit as you see fit and we can review]

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

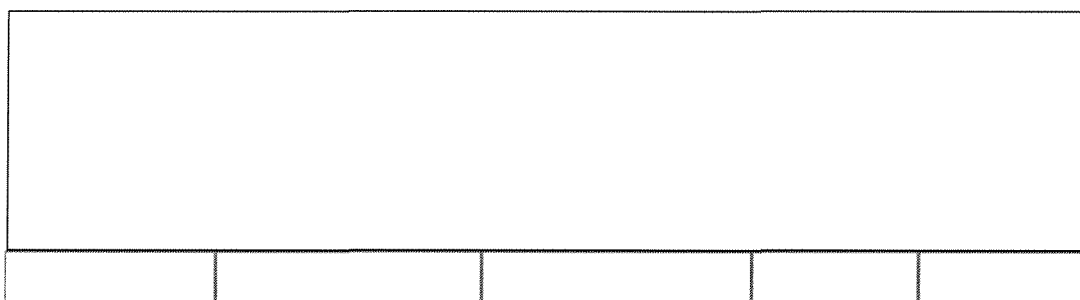
Fw: UPDATE ON COMPUTER HACKING - Please Read

Veldran, Katherine

Sent: Friday, October 26, 2012 7:27 PM**To:** Veldran, Katherine

From: Rep. Bill Taylor [mailto:bill@taylorschouse.com]
Sent: Friday, October 26, 2012 07:25 PM
To: Veldran, Katherine
Subject: UPDATE ON COMPUTER HACKING - Please Read

You're receiving this email because of your relationship with **TaylorSCHouse**. You may **unsubscribe** if you no longer wish to receive our emails.



SC's Computer Hacking Update

(Informational Newsletter)

UPDATE

The web link provided in the initial 'Hacker' newsletter doesn't seem to be useful. That web address, which was provided by the Governor's office and is being used by the news media, delivers you to a page that asks for an activation code.

We're told you have to call 866-578-5422 to get the activation code. Of course, the phones lines are so jammed, as one would expect in an event like this, you get a recording asking you to call back later.

It appears patience is the best prescription at the moment.
I'll send out updates as we learn more.



This email was sent to katherineveldran@gov.sc.gov by bill@taylorschouse.com |
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).



Bill Taylor for SC House District 86 | P.O. Box 2646 | Aiken | SC | 29801

Fw: From the Governor's Office re. cyber-attack at DOR

Veldran, Katherine

Sent: Friday, October 26, 2012 7:05 PM

To: Veldran, Katherine

From: Larry Martin [mailto:lmartin@alicemfgco.com]

Sent: Friday, October 26, 2012 07:04 PM

To: Schimsa, Rebecca

Cc: Pitts, Ted; Veldran, Katherine

Subject: Re: From the Governor's Office re. cyber-attack at DOR

Not suggesting you reply to my comment this evening, but just want to report that protectmyid.com/scdor simply takes you to the default homepage of protectmyid.com . I tried it a couple of time and it doesn't take you to the scdor page.

Thanks!

Larry

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

From: Schimsa, Rebecca

Cc: Pitts, Ted ; Veldran, Katherine

Sent: Friday, October 26, 2012 4:44 PM

Subject: From the Governor's Office re. cyber-attack at DOR

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.

-###-

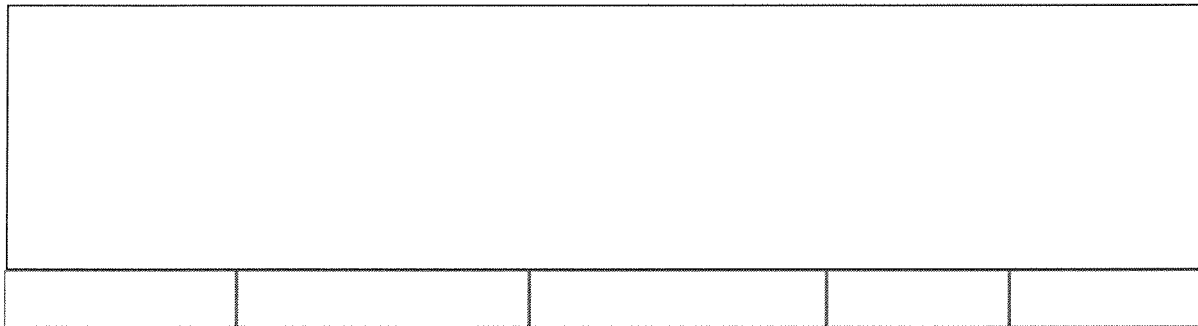
Fw: SC 's Been HACKED - This is a serious warning OPEN NOW

Veldran, Katherine

Sent: Friday, October 26, 2012 6:45 PM**To:** Veldran, Katherine

From: Rep. Bill Taylor [mailto:bill@taylorschouse.com]**Sent:** Friday, October 26, 2012 06:25 PM**To:** Veldran, Katherine**Subject:** SC 's Been HACKED - This is a serious warning OPEN NOW

You're receiving this email because of your relationship with **TaylorSCHouse**. You may **unsubscribe** if you no longer wish to receive our emails.



SC's Been HACKED !

(Informational Newsletter)

Dear Friends:

You may have heard the late breaking news that your identity may be at risk.

The SC Department of Revenue revealed this afternoon that they experienced a cyber attack and approximately **3.6 million Social Security numbers and 387,000 credit and debit card numbers** have been exposed. I've been receiving calls from folks concerned they may be a victim. Those concerns are justified. 3.6 million Social Security numbers includes most of us. The vast majority of credit cards on file with the Revenue Department are protected by strong encryption, but about **16,000 are unencrypted**.

The state says the cyber hole has been plugged, but you have every right to be concerned and take steps now to protect yourself from identity theft or misuse of your credit or debit card.

Here's what you need to do...

1. Anyone who has filed a South Carolina tax return since 1998 is urged to visit protectmyid.com/scdor or **call 866-578-5422** to determine if their information is affected. (Expect long wait times on the phone call.) Phone will be answered until 9:00 pm and will be open again tomorrow.

2. To protect taxpayers, the state will provide those affected with one year of credit monitoring and identity theft protection.

3. In addition to the Experian monitoring 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.

Additional steps to protect yourself...

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.

Final Thought

This is a most serious and regrettable situation that puts you at risk. Legislators will be briefed Monday morning and I'll report back. In the meantime, I urge each of you to be on alert and take the necessary steps to protect your identity, credit and banking information.

In your Service,

Bill Taylor

803-270-2012

Representative
South Carolina General
Assembly

Bill@taylorschouse.com

www.Taylorschouse.com

Newsletter not paid for by
taxpayer funds.

Paid for by TaylorSCHouse



This email was sent to katherineveldran@gov.sc.gov by bill@taylorschouse.com |
[Update Profile/Email Address](#) | Instant removal with [SafeUnsubscribe™](#) | [Privacy Policy](#).

Bill Taylor for SC House District 86 | P.O. Box 2646 | Aiken | SC | 29801

Fw: A new message from Tommy Pope

Veldran, Katherine

Sent: Friday, October 26, 2012 6:45 PM

To: Veldran, Katherine

From: Tommy Pope via Rally [mailto:team@rally.org]

Sent: Friday, October 26, 2012 05:00 PM

To: Veldran, Katherine

Subject: A new message from Tommy Pope

UPDATE FROM

Tommy Pope



Share this



Post a comment

via

RALLY

The South Carolina Department of Revenue announced today that they experienced a security breach. Approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Although the majority of the credit cards are protected by strong encryption, approximately 16,000 are unencrypted.

The state intends to provide those affected with one year of credit monitoring and identity theft protection. No public funds were accessed or put at risk.

According to a press release from the Department of Revenue, "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."

To learn more about the security breach and additional steps to protect your identity and financial information, view the press release here:
<http://www.sctax.org/NR/rdonlyres/5AF6995A-F9F0-42E7-A430-EC620CCE8C7D/0/1DORmediarelease.pdf>

[continue reading]

Give Now

Tommy Pope has 1116 supporters like you.



Manage email frequency or
unsubscribe from further updates.
You can also get a weekly digest.



Fundraise for any cause

with Rally's free, social fundraising tools.

What do you rally for?

Rally.org 144 Second Street, San Francisco, CA 94105

Recording

Ozzie Fonseca [ofonseca@experianinteractive.com]

Sent: Friday, October 26, 2012 5:19 PM

To: Stirling, Bryan

I'm still trying to track down my call center contact to get status. I'll send you an update as soon as I can.

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

Blog: www.Experian.com/blogs/data-breach
Follow us on Twitter: 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.

legislator notifications

Schimsa, Rebecca

Sent: Friday, October 26, 2012 4:47 PM

To: Pitts, Ted; Veldran, Katherine; Stirling, Bryan; Godfrey, Rob

Cc: Haltiwanger, Katherine; Soura, Christian

This afternoon at 4:45 p.m., an email went out to members of the General Assembly including:

1. Media release from our office;
2. Media release from DOR;
3. Video of today's press conference; and
4. Conference call information for Monday.

Thanks.

Rebecca S. Schimsa
Office of Governor Nikki R. Haley
Staff Attorney & Commerce Liaison
O: (803) 734-6068 | C: (803) 429-4561

UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Godfrey, Rob

Sent: Friday, October 26, 2012 4:27 PM

Importance: High

Attachments: Media_Release_10262012.pdf (1 MB)

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.

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

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

Godfrey, Rob

Sent: Friday, October 26, 2012 3:06 PM

Attachments: Media_Release_10262012.pdf (1 MB)

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.

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

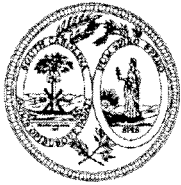
- Regularly review credit reports;
- Place fraud alerts with the three credit bureaus;
- Place a security freeze on financial and credit information with the three credit bureaus.

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



State of South Carolina
Department of Revenue
300A Outlet Pointe Blvd., Columbia, South Carolina 29210
P.O. Box 125, Columbia, South Carolina 29214

C-450 (Rev. 8/29/12) 6371

For Immediate Release:

October 26, 2012

Contact: Rob Godfrey

Office of Gov. Nikki Haley

(803) 734-5074 (803) 429-5086

Samantha Cheek

SC Department of Revenue

(803) 898-5281

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 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.

"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."

###

Chronology

October 10:

- The SC Department of Revenue was informed by the South Carolina Division of Information Technology (DSIT) of a potential cyber attack involving the personal information of taxpayers.
- DOR worked with DSIT throughout the day to determine what may have happened and what steps needed to be taken immediately to deal with the situation.
- DOR consulted with state and federal law enforcement agencies for guidance.
- Law enforcement recommended several steps to be taken, including consulting the nation's top cyber security firms.
- DOR assessed the top 3 recommendations from law enforcement and contacted Mandiant of Alexandria, VA.
- DOR contacted the Governor's office.
- SLED Chief Keel briefed Governor Haley.

October 11:

- DOR met with the Governor's office in the morning to give her a full briefing, including laying out our 4-pronged approach:
 - Contract with Mandiant, which we signed on October 12 with the approval of the Governor, to find and fix the leak;
 - Conduct an internal investigation of all outside contractors and certain employees to see if they have been involved with any security breaches;
 - Develop of a public notification plan;
 - Institute additional protection tools on our system.
- DSIT began monitoring DOR and its main servers to detect any unauthorized intrusions.
- DOR made the decision that if DSIT or DOR identified any unusual exfiltrations of data, the system impacted would be shut down immediately.

October 12:

- DOR signed a contract with Mandiant.
- Mandiant began working on plans to send surveillance and monitoring tools to be installed at DOR in SC.

October 15:

- DOR worked with Mandiant to begin installing surveillance and monitoring equipment which was completely in place within 48 hours.
- DOR began daily status update calls with complete team, including representatives from law enforcement, DSIT, DOR, Mandiant- the first call was planning session.

October 16:

- Mandiant began deploying a monitoring agent on every computer workstation throughout DOR, a process was completed by October 20.

- By the daily status call on Oct. 16, Mandiant was able to confirm that an unknown hacker or hackers probed the system in early September. We also learned that in mid-September, two other intrusions occurred, and to the best of our knowledge, the hacker obtained data for the first time.

October 18:

- Daily team status meetings were held and systems were continuously monitored.

October 19:

- Mandiant sent a four member team to begin the on-site investigation at DOR.
- DOR is still managing day-to-day business of state of SC while managing this major issue.
- DOR contacted South Carolina law firm, Nelson Mullins, about getting assistance with breach management.

October 20:

- The “hole” was closed and system was secured, to the best of our current knowledge.

October 21-25:

- We continued to monitor the system to make sure no more data was compromised.
- 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.
- We confirmed that NO public funds were accessed or put at risk as those servers are completely separate from those that were breached.
- However, approximately 3.6 million Social Security numbers may be affected. Approximately 387,000 credit card numbers were in the materials that were taken, but approximately 371,000 are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders, and the others are dated from before 2003.

Safety Precautions:

- We are taking immediate steps to protect the taxpayers of South Carolina, including providing one year of credit monitoring to those who may be affected through Experian’s ProtectMyID Alert. This service includes:
 - A free credit report;
 - Daily credit monitoring across three credit bureaus to detect any suspicious activity;
 - A \$1 million identity theft insurance policy.
- The public is urged to be aware of scams. DOR will never call or otherwise contact those affected asking for personal information. Beneficiaries are advised to never give out their Social Security numbers or other identifying information to people you do not know.
- If you filed a South Carolina tax return since 1998, you are urged to call the toll-free call center that DOR has established, which will be operating 24/7 beginning at noon on Friday, October 26, 2012, for anyone who wishes to know if their personal information was included and to immediately enroll in one year of credit monitoring: 1-866-578-5422. Also please visit: ProtectMyID.com/SCDOR.
- Please see list of additional Consumer Safety Solutions.

Consumer Safety Solutions

You can help prevent your information from being misused by taking some of the following simple steps.

In addition to these steps, the South Carolina Department of Revenue will be protecting the taxpayers of South Carolina, by providing one year of credit monitoring to those who may be affected through Experian's ProtectMyID Alert. This service includes:

- A free credit report;
- Daily credit monitoring to detect suspicious activity;
- A \$1 million identity theft insurance policy.

The public is urged to be aware of scams. DOR will never call or otherwise contact those affected asking for personal information. Beneficiaries are advised to never give out their Social Security numbers or other identifying information to people you do not know.

If you filed a South Carolina tax return since 1998, you are urged to call the toll-free call center that DOR has established, which will be operating 24/7 beginning noon on Friday, October 26, 2012, for anyone who wishes to know if their personal information was included and to immediately enroll in one year of credit monitoring: 1-866-578-5422. Also please visit ProtectMyID.com/scdor for more information.

1. Review Your Credit Reports and Bank Statements. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. You can receive free credit reports by placing fraud alerts and through your credit monitoring. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement.

2. Contact Credit/Debit Card Issuer. When credit/debit card information is compromised, the best protection is reissue of the card. So to protect yourself from the possibility of unauthorized charges, we recommend that you check your bank account statements regularly. If you detect any

unauthorized charges, we strongly suggest that ***you contact your credit/debit card issuer immediately by calling the toll-free number located on the back of your card or on your monthly statement, tell them what you have seen, and ask them to cancel and reissue the card.*** You should tell your credit/debit card issuer that your account may have been compromised and review all charges on your account for potentially fraudulent activity. We also recommend that you change your credit/debit card web account password immediately when you discover unauthorized charges.

3. Place Fraud Alerts with the three credit bureaus. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-800-525-6285
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9532
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review.

4. Security Freeze: By placing a freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above in writing to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. In South Carolina, there is no charge to you for placing, thawing or lifting the freeze.

Credit Bureaus

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze

TransUnion Fraud Reporting
1-800-680-7289
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
<http://freeze.transunion.com>

5. You Can Obtain Additional Information about the steps you can take to avoid identity theft from the following:

For South Carolina Residents:

South Carolina Office of the Attorney General
The Honorable Alan Wilson
P.O. Box 11549
Columbia, S.C. 29211
1-803-734-3970
www.scag.gov

South Carolina Department of Consumer Affairs:
1-800-922-1594 (Toll-Free)
803-734-4200
scdca@scconsumer.gov
Mailing Address:
PO Box 5757
Columbia SC 29250-5246
www.consumer.sc.gov

For all U.S. Residents:

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TDD: 1-202-326-2502

Talking points gov DOR SLED presser

Pitts, Ted

Sent: Friday, October 26, 2012 12:15 PM

To: LeMoine, Leigh; Stirling, Bryan; Godfrey, Rob

Attachments: Talking points gov DOR SL~1.docx (19 KB)

Gov. Haley Talking Points

- The State of South Carolina is the victim of a crime committed by a very sophisticated hacker.
- On October 10th South Carolina Department of Revenue and SLED were notified that a server that warehouses taxpayer data was breached and copies of taxpayer information was stolen.
- For the last two week's State and Federal law enforcement agencies and SCDOR have been working around the clock on this case.
- We can report that the access point used to access the information has been plugged, SC DOR and it's computer forensic experts have determined what information was compromised and the system is now secure.
- Our State will respond to this crime with an unprecedented, large-scale plan.
- I have ordered Jim Etter and SCDOR to take every means necessary to protect South Carolina's taxpayers. A part of this protection is that every taxpayer can sign up for one year of identity theft protection and credit monitoring. All they have to do is call the 1800 number.
- 1) Call Center- By calling the 1800 number taxpayers can have any questions answered.
- 2) Credit Protection- While we do not believe every taxpayer's information has been exposed, out of an abundance of caution, the state is prepared to offer this protection to any taxpayer who has filed a return with our State since 1998.
- 3) Holistic look and approach by IG- In this day and age, cyber-security is a paramount concern, and we must make every effort to protect ourselves. Because of this, I have asked our State's Inspector General to lead the effort in looking at all of our State IT systems in a holistic view and make recommendations to State leaders on how we can assure we have limited our vulnerabilities.
- I have confidence that Jim Etter and Department of Revenue are working diligently to take the right steps in this constant battle with an evolving information and technology environment we live in.
- I also have confidence in Chief Keel, SLED and our Federal partners as they continue to investigate this matter.
- I cannot emphasize enough that if you have filed a tax return since 1998, it is important that you call the 800 number or visit the website today to find out if your information is at risk and how to protect yourself.