## Godfrey, Rob

**From:** Jon Neiditz <Jon.Neiditz@nelsonmullins.com>
**Sent:** Friday, October 26, 2012 8:17 AM
**To:** Tim Kelly; Godfrey, Rob; Rick Silver; Jim Etter; Harry Cooper; Samantha Cheek; Liz Mason
**Cc:** Rush Smith; ofonseca@experianinteractive.com
**Subject:** RE:

But you tweet well, which puts you ahead of most, Tim. Excellent work, everyone! No changes from me. Having a working call center of well-trained professionals that can handle high volumes by 8:00 a.m. Pacific Time will make this go 10 times as well as it would have otherwise. Make sure you share expectations regarding escalation of calls; Experian's experiance in the State should be helpful.

Regarding the press conference, I would anticipate that the law enforcement involvement will be a silent 800 pound gorilla in the room. Once you get through the press conference, please reconnect with me on the alternative notice, on which I am working.

Congratulations (knock on wood), thanks and best,

Jon


Nelson Mullins

Jon A. Neiditz
Partner
jon.neiditz@nelsonmullins.com

Nelson Mullins Riley & Scarborough LLP
Atlantic Station
201 17th Street NW, Suite 1700
Atlanta, GA 30363
Tel: 404.322.6139 Fax: 404.322.6033
www.nelsonmullins.com
(View Bio)


**From:** Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
**Sent:** Friday, October 26, 2012 7:49 AM
**To:** Godfrey, Rob; Rick Silver; Jim Etter; Harry Cooper; Samantha Cheek; Liz Mason
**Cc:** Rush Smith; Jon Neiditz; ofonseca@experianinteractive.com
**Subject:**

Media package contents are attached, including the formatted press release. I'll need any changes to the release by 9:15 am in order to assemble the press kits. If there are no changes to the other documents, I'm going to print those at 8:30 come hell or high water.

Thanks to everyone for your patience and professionalism, two qualities I rarely display myself!

TK

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

1411 Gervais Street
Columbia, SC 29201


- Follow Chernoff Newman

## Godfrey, Rob

**From:** Harry Cooper <COOPERH@sctax.org>
**Sent:** Friday, October 26, 2012 10:21 AM
**To:** Jon Neiditz; Tim Kelly; Godfrey, Rob; Rick Silver; Jim Etter; Samantha Cheek; Liz Mason
**Cc:** Rush Smith; ofonseca@experianinteractive.com
**Subject:** RE:

...yes well done team! Thanks.

**From:** Jon Neiditz [mailto:Jon.Neiditz@nelsonmullins.com]
**Sent:** Friday, October 26, 2012 8:17 AM
**To:** Tim Kelly; Godfrey, Rob; Rick Silver; Jim Etter; Harry Cooper; Samantha Cheek; Liz Mason
**Cc:** Rush Smith; ofonseca@experianinteractive.com
**Subject:** RE:

But you tweet well, which puts you ahead of most, Tim. Excellent work, everyone! No changes from me. Having a working call center of well-trained professionals that can handle high volumes by 8:00 a.m. Pacific Time will make this go 10 times as well as it would have otherwise. Make sure you share expectations regarding escalation of calls; Experian's experiance in the State should be helpful.

Regarding the press conference, I would anticipate that the law enforcement involvement will be a silent 800 pound gorilla in the room. Once you get through the press conference, please reconnect with me on the alternative notice, on which I am working.

Congratulations (knock on wood), thanks and best,

Jon

Nelson Mullins

Jon A. Neiditz
Partner
jon.neiditz@nelsonmullins.com

Nelson Mullins Riley & Scarborough LLP

Atlantic Station
201 17th Street NW, Suite 1700
Atlanta, GA 30363
Tel: 404.322.6139 Fax: 404.322.6033

www.nelsonmullins.com
(View Bio)

**From:** Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
**Sent:** Friday, October 26, 2012 7:49 AM
**To:** Godfrey, Rob; Rick Silver; Jim Etter; Harry Cooper; Samantha Cheek; Liz Mason
**Cc:** Rush Smith; Jon Neiditz; ofonseca@experianinteractive.com
**Subject:**

Media package contents are attached, including the formatted press release. I'll need any changes to the release by 9:15 am in order to assemble the press kits. If there are no changes to the other documents, I'm going to print those at 8:30 come hell or high water.

Thanks to everyone for your patience and professionalism, two qualities I rarely display myself!

TK

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

1411 Gervais Street
Columbia, SC 29201

- Follow Chernoff Newman

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 5:58 PM
**To:** 'Greg.Young@experianinteractive.com'
**Cc:** Stirling, Bryan
**Subject:** Re: Experian PR contact

What are y'all providing to the P and C?

----- Original Message -----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Saturday, October 27, 2012 02:47 PM
To: Godfrey, Rob
Subject: RE: Experian PR contact

Got it

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

-----Original Message-----
From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Saturday, October 27, 2012 11:43 AM
To: Greg Young; Stirling, Bryan
Subject: Re: Experian PR contact

Greg -- Diette Courrege, The Charleston Post and Courier, 8439375546 dcourrege@postandcourier.com

----- Original Message -----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, October 26, 2012 10:48 PM
To: Stirling, Bryan

Cc: Godfrey, Rob
Subject: RE: Experian PR contact

Rob -

We'll be sending a statement out to you in the very near future; just wordsmithing a couple items. I understand the late night news is about to kick in, and we may miss that window, but again -- want to say this correctly and communicate that we are in control.

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

-----Original Message-----
From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Friday, October 26, 2012 5:59 PM
To: Greg Young
Cc: Godfrey, Rob
Subject: RE: Experian PR contact

Greg,
Please send us that statement so Rob can look at it and decide how to handle.
Thank you.

-----Original Message-----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, October 26, 2012 7:38 PM
To: Stirling, Bryan
Subject: Re: Experian PR contact

Bryan,

Still on call. Have some message points but getting more. Apologies for delay.

GY

Greg Young, APR
Experian Consumer Direct
Director, Public Relations /Consumer Engagement
949-294-5701

Sent by my iPhone

On Oct 26, 2012, at 3:48 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

That works for me. Thank you.

-----Original Message-----
From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 6:47 PM
To: Stirling, Bryan
Cc: Ozzie Fonseca; Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Bryan:

As long as the call center is recording the message, I would suggest stating that people have until January 31st ,2013 to request an activation code. If that works for you I'll have them add that language immediately.

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

Blog: www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-breach><http://www.Experian.com/blogs/data-breach>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR><http://www.Twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach

"Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

Thank you.

-----Original Message-----
From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 6:35 PM
To: Stirling, Bryan
Cc: Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Bryan:

I spoke with our call center and they found a way to record the message in eastern terms. That will be done within the next 60 minutes.

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

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

Blog: www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-breach><http://www.Experian.com/blogs/data-breach>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR><http://www.Twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach



-----Original Message-----
From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Friday, October 26, 2012 3:23 PM
To: Ozzie Fonseca
Cc: Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Thank you, call him now.

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

From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 6:22 PM
To: Stirling, Bryan
Cc: Greg Young; Thad Westbrook
Subject: Experian PR contact

Bryan:

Here is our PR contact:

Greg Young
949 567-3791
Greg.Young@experianinteractive.com<mailto:Greg.Young@experianinteractive.com>

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

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

Blog: www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-breach><http://www.Experian.com/blogs/data-breach>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR><http://www.Twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 6:36 PM
**To:** 'Greg.Young@experianinteractive.com'
**Cc:** Stirling, Bryan
**Subject:** Re: Experian PR contact

Thanks.

----- Original Message -----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Saturday, October 27, 2012 06:29 PM
To: Godfrey, Rob
Cc: Stirling, Bryan
Subject: RE: Experian PR contact

We are getting together a response on about 10 questions she threw into one email. Will run response by you first.

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

-----Original Message-----
From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Saturday, October 27, 2012 2:58 PM
To: Greg Young
Cc: Stirling, Bryan
Subject: Re: Experian PR contact

What are y'all providing to the P and C?

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

From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Saturday, October 27, 2012 02:47 PM
To: Godfrey, Rob
Subject: RE: Experian PR contact

Got it

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

-----Original Message-----
From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
Sent: Saturday, October 27, 2012 11:43 AM
To: Greg Young; Stirling, Bryan
Subject: Re: Experian PR contact

Greg -- Diette Courrege, The Charleston Post and Courier, 8439375546 dcourrege@postandcourier.com

----- Original Message -----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, October 26, 2012 10:48 PM
To: Stirling, Bryan
Cc: Godfrey, Rob
Subject: RE: Experian PR contact

Rob -

We'll be sending a statement out to you in the very near future; just wordsmithing a couple items. I understand the late night news is about to kick in, and we may miss that window, but again -- want to say this correctly and communicate that we are in control.

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

-----Original Message-----
From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Friday, October 26, 2012 5:59 PM
To: Greg Young
Cc: Godfrey, Rob
Subject: RE: Experian PR contact

Greg,
Please send us that statement so Rob can look at it and decide how to handle.
Thank you.

-----Original Message-----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, October 26, 2012 7:38 PM
To: Stirling, Bryan
Subject: Re: Experian PR contact

Bryan,

Still on call. Have some message points but getting more. Apologies for delay.

GY

Greg Young, APR
Experian Consumer Direct
Director, Public Relations /Consumer Engagement
949-294-5701

Sent by my iPhone

On Oct 26, 2012, at 3:48 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

That works for me. Thank you.

-----Original Message-----
From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 6:47 PM
To: Stirling, Bryan
Cc: Ozzie Fonseca; Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Bryan:

As long as the call center is recording the message, I would suggest stating that people have until January 31st ,2013 to request an activation code. If that works for you I'll have them add that language immediately.

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

Blog: www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-breach><http://www.Experian.com/blogs/data-breach>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR><http://www.Twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach



"Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

Thank you.

-----Original Message-----
From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 6:35 PM
To: Stirling, Bryan
Cc: Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Bryan:

I spoke with our call center and they found a way to record the message in eastern terms. That will be done within the next 60 minutes.

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

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

Blog: www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-breach><http://www.Experian.com/blogs/data-breach>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR><http://www.Twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach



-----Original Message-----
From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Friday, October 26, 2012 3:23 PM
To: Ozzie Fonseca
Cc: Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Thank you, call him now.

-----Original Message-----
From: Ozzie Fonseca [mailto:ofonseca@experianinteractive.com]
Sent: Friday, October 26, 2012 6:22 PM
To: Stirling, Bryan
Cc: Greg Young; Thad Westbrook
Subject: Experian PR contact

Bryan:

Here is our PR contact:

Greg Young
949 567-3791
Greg.Young@experianinteractive.com<mailto:Greg.Young@experianinteractive.com>

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

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

Blog: www.Experian.com/blogs/data-breach<http://www.Experian.com/blogs/data-breach><http://www.Experian.com/blogs/data-breach>
Follow us on Twitter:
www.Twitter.com/Experian_DBR<http://www.Twitter.com/Experian_DBR><http://www.Twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Wednesday, October 24, 2012 4:46 PM
**To:** 'tcsmith@greenvillenews.com' (tcsmith@greenvillenews.com)
**Subject:** Tim, the Inspector General is going to call you regarding his work with the governor to secure our state's computer systems.

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Wednesday, October 24, 2012 5:14 PM
**To:** 'tcsmith@greenvillenews.com' (tcsmith@greenvillenews.com)
**Subject:** Letter from IG to the governor
**Attachments:** Summary Letter to Governor_Agcy_Data_Sec.docx

# State of South Carolina
## Office of the Inspector General

September 18, 2012

Honorable Nikki R. Haley
Governor of South Carolina
1205 Pendleton Street
Columbia, SC 29201

Re: Status Update - Review of Information Security at the Cabinet Agencies

Dear Governor Haley,

The Office of the Inspector General (OIG) has reviewed the information security practices at 12 of the 16 Cabinet Agencies. The Department of Health & Human Services (DHHS) was not included in the review inasmuch as a consultant has been retained to perform a similar, if not more extensive, evaluation. The OIG will complete its review by early October, 2012.

Of the 12 agencies evaluated, three were found either not to retain any Personally Identifiable Information (PII) other than a minimal amount constituting a minimal risk, or information retained is considered a public record under the State's public record statutes. The remaining nine agencies reviewed to date are in substantial compliance with sound information security practices. It was clear from the review, information security awareness has been heightened throughout the Cabinet Agencies since the April, 2012 DHHS data breach, and agency leadership is proactively engaged in ensuring an adequate information security posture.

Based on recommended security guidelines and best practices in government and the private sector, a questionnaire was developed to test nine major information security categories in each agency against best practices. The questionnaire was completed for each agency and interviews were conducted with employees at different levels within each agency. In some cases, the OIG viewed facilities and observed business processes. These nine categories were:

- Information Security Policy and Other IT Policies
- Inventory/Discovery of PII
- Inventory and Monitoring of Network Devices and Activity
- Password Management
- Workstation, Laptop and Other IT Devices – Setup & Security
- Database Permissions, User Management and Application Security

OFFICE OF THE INSPECTOR GENERAL • KINGSTREE BUILDING • 110 CENTERVIEW DRIVE, SUITE 201 • COLUMBIA, SOUTH CAROLINA 29210
OFFICE: 803.896.4729 • FAX: 803.896.4309 • EMAIL: OIG@OIG.SC.OIG • TOLL-FREE HOTLINE: 1.855.SCFRAUD (1.855.723.7283)

September 18, 2012
Governor Nikki R. Haley

- Employee Information Security Awareness Training
- Data Loss Protection Tools and Monitoring of Network Activity
- Data Loss Response Plan

Despite all nine agencies being in substantial compliance, the OIG identified three areas with a pattern of non-compliance where information security could be improved. Those areas are as follows:

1. Lack of adequate security for the paper records containing confidential information (4 of the 9 agencies could improve).

2. Lack of a process to periodically conduct an agency-wide discovery process to assure that the locations of all confidential information are known and authorized (8 of the 9 agencies could improve). Most, if not all, agencies expressed confidence that all locations of confidential information were known and authorized, yet these agencies had not undertaken such a process, or at least, had not done so periodically. Periodically conducting an agency-wide discovery process is a major industry recommended best practice.

3. Lack of a data response plan along with a standing committee to execute it should such an information loss occur (7 of the 9 agencies could improve). This is also a major industry recommended best practice.

Agency Directors and their personnel demonstrated commitment to address these areas to improve. Each agency will receive a separate report on its information security, along with corresponding findings and recommendations. Each agency was accommodating and helpful to the OIG in conducting this review, and it was a pleasure working with them. If you or your staff needs any additional information or clarification, please do not hesitate to call me at (803) 896-4721.

Sincerely,

Patrick J. Maley
Inspector General

PM/pw

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Wednesday, October 24, 2012 5:18 PM
**To:** 'tcsmith@greenvillenews.com' (tcsmith@greenvillenews.com)
**Subject:** Agency follow up
**Attachments:** Confidentiality Regs-Policies.pdf

**Importance:** High

**Department of Commerce:**

The South Carolina Department of Commerce updated its confidentiality agreement with all of our employees to include social media. In addition, employees will sign a new agreement every year as part of their EPMS process.

In June of 2012, our agency met with an auditor from the Inspector General's Office working on a security project for the Governor's Office. He indicated that Commerce did not maintain personal information and was outside the scope of his current review.

Thanks and let me know if you have any questions.

Chris Huffman
Chief Financial Officer
South Carolina Department of Commerce
1201 Main Street, Suite 1600
Columbia, SC 29201
803.737.0462 Office
803.553.4875 Cell

**PPP:**

SCDPPPS has jurisdiction over more than 32,000 criminal offenders who are on probation, parole or other forms of supervision. Records are maintained on all of them, as well data on previous offenders who are no longer under the Department's supervision. Some of the data are public by law (sentences and convictions), and confidential (SSNs, victim and family names).The Department has policies, procedures and software in place to protect the disclosure of the confidential data. The Department is committed to ensuring the integrity and safety of its data and data system by continuously assessing and enhancing its security measures. Some of those protection measures include internal and external systems such as:

Current Internal / External Protocols

- Department personnel may only access the data system upon granting of security level rights. The restricted rights are based on the employee's role and level of responsibility within the Department. Rights are granted through a multi-step approval process involving supervisors and the Department's Strategic Development and Information Technology (SDIT).
- The Department maintains a designated SDIT staff person responsible for monitoring system security. This monitoring includes, but is not limited to: viruses, malware, system breaches, assessment of internal use patterns, etc.
- The Department maintains multiple system monitoring strategies, to include but not limited to: firewalls, networking inspection appliances, network monitoring, and data loss protection systems.

Data Authorization / Control

The Department maintains strict protocols for managing the release of data.

- All data provided in electronic format is encrypted and requires additional security protocols for the user to access.
- The Department maintains written agreements with law enforcement entities for the release of requested data.
- Data released to non-law enforcement entities require a specific request that is reviewed for purpose, data range, etc., prior to being considered for release.
- Department maintains a formal data request process for internal and external customers. Each request is outlined and submitted for review by Divisional Management before being approved. All data requests require the approval of the Director before being approved.

Pending Strategies to Enhance Data Security

- In conjunction with the Governor's strategy to enhance data security, the Department has participated with the Inspector General's Office to conduct a review of its data security system.
- The Department is scheduled to migrate to a Microsoft platform in early 2013 and this will allow for significant security enhancements and the implementation of a two (2) factor authentication model.
- The Department is pending implementation of annual security awareness training for all staff.

**DPS:**

SCDPS - Personal Protection / Securing Data

SCDPS' status as a law enforcement agency requires us to establish clear and explicit standards on appropriate and acceptable uses of our computer resources and information systems.

Because of DPS's law enforcement responsibility, the department's "network" and information systems adhere to standards set forth in the Commission on Accreditation for Law Enforcement Agencies (CALEA). We are inspected (reaccredited) every 3 years.

DPS accepts and maintains CJIS (Criminal Justice Information Systems) Security Policy as the minimum level of security requirements acceptable for the transmission, processing, and storage of the nation's CJIS data.

DPS meets all SLED, CJIS, FBI, NCIC, and NLETS Security and Technical requirements. (Criminal History information.)

DPS has numerous policy Directives in place to address securing data issues: Computer Privacy Policy, Password Security, Information Technology, Appropriate Use of Computer Resources, Network and Information Systems Management, Records Management, and Release of Information Policies.

DPS also issued a "Special Directive/Policy" on the Storing of Sensitive Equipment. Equipment items, especially laptops and vehicle consoles, contain sensitive information. Great care will be taken when the equipment remains in an unattended vehicle used by department personnel in the performance of their duties.

Our Office of Information Technology (OIT) is charged with assuring the integrity of the Department's network and its information systems by utilizing several requirements (Access controls; Utilizes password security systems; Routinely monitors users' accounts; and Audit trail of computer activity, etc.) Additionally, the OIT utilizes several other measures such as:

- SCDPS has a system to alert IT personnel if an intrusion of an unidentified source tries to gain access to our system.
- The computer operating system is automatically locked after 15 minutes without any user activity.
- SCDPS members are prohibited from sharing passwords.
- All access is password protected.
- Access to Human Resource data is largely administered by the State OHR and SCEIS. Very few personnel with SCDPS have access to this data.

**DEW:**

We perform the following functions as part of normal business process to prevent PII data loss:

Network and Data Security --

- All text email sent from the Agency is automatically scanned for PII - specifically data that appears to be SSNs, credit cards.
- Unauthorized email to a large distribution group is automatically restricted.
- Large emails are prevented from being sent outside the Agency until the email is verified by a human to be valid for work use.
- Tools and devices are in place that prevent malicious hacking of our network and web applications and databases
- Laptops used by agents in the field are encrypted in case of loss

Awareness Training --

- All employees are required to take IT security training as part of their onboarding that specifically informs of the proper use and protection of PII.
- All employees are required to read and acknowledge security policies, procedures to include acceptable use of PII

Physical Protection --

- Sensitive areas with PII are accessed by key card only

Actions taken after the DHHS breach:

- All remote access by employees is secured using best practice authentication measures ("two-factor authentication")
- Controls have been implemented to ensure that access to mainframe and other applications is promptly revoked for DEW staff when they terminate employment.
- IT is scanning computers in the SCWorks centers for files containing PII.
- Upgraded the network infrastructure with modern and more secure components (routers, switches).
- Additional security measures and physical controls (sign in log, locked containers) were implemented for the warehouse to increase security over stored paper documents.
- A system configuration issue with the email filter (detecting SSNs) was identified and corrected.
- Hard drives from all computer equipment that will be transferred to State Surplus Property, or disposed of in any other way, are now being removed and destroyed by IT staff prior to the computers being transported to the DEW warehouse.

Because of the Agency re-organization, the following additional steps were taken last week to protect the Agency from possible malicious intent:

- Flagged email that seemed suspicious for affected employees. Follow up to be conducted by IT. Suspicious emails may include those that have large attachments, odd subject lines, or are being sent to outside email addresses (media, etc)
- Audits of application and data access for the affected employees to ensure it was necessary for job duties.

Please let me know if you have any questions.

Joe

**PRT**

1. Removed employee SSN from all HR / personnel paperwork (EPMS, leave forms, etc).

2. When selected vendors for point-of-sale and reservation system required that they be PCI compliant. (We do not capture or store any credit card numbers – all information is encrypted and sent to vendors.)

**SCDHHS:**

Following the Medicaid data breach in April 2012, SCDHHS took several significant steps to alter the way data, including personal health information (PHI) and personally identifiable information (PII) is accessed and managed within the agency.

The following policies and procedures have been updated based on this incident:

DATA ACCESS AND SECURITY POLICIES

Restricted access to data and data warehouse to align access to employee duties (April, 2012)

Limit data access to what employee needs to complete job (April, 2012)

Updated policies for granting access to data and data warehouse (April, 2012)

Added functionality to data warehouse to mask PHI/PII by default (May, 2012)

Delivered new tool for program integrity (internal audit) to sample/audit emails

SYSTEMS CHANGES

Updated email infrastructure (modernized email system, July, 2012)

Changes to email system to encrypt email communications whenever possible (forced and automated, July, 2012)

Updated tools to identify potential PHI/PII in email content/body (July, 2012)

Piloting solution to identify potential PHI/PII in email attachments (in-progress)

TECHNICAL SYSTEMS REVIEW

Engaged external security experts (SECNAP) to deliver technical assessment and recommendations for infrastructure and security (in-progress)

DATA MANAGEMENT PROCESS REVIEW

Engaged external security experts (Gartner) to deliver assessment and recommendations for data, process and system related security, compliance and risk (in-progress)

CRISIS MANAGEMENT PLAN

Completed internal assessment of handling of data release and recommendations for crisis management plan (August 2012)

Implementation of recommendations for crisis management planning and team identification (in-progress)

RELATED PERSONELL POLICIES AND TRAINING

Updated HIPAA Policy — Beginning May 2012, the HIPAA policy has been changed from being a one-time training at hire/orientation to an annual review/update by all employees.

Conflict of Interest/Outside Employment — The agency implemented an Outside Employment Policy and it is now included in the employee orientation. This policy is designed to deter employees from improperly benefitting from their position and/or the data they may have access to at SCDHHS.

**SCDMV:**

SCDMV has taken the following measures to prevent data theft from an internal threat:

1. We disabled USB ports that provide thumb drive access to our computers. That said, we do have a few specific personnel who retain that capability (less than 20 - primarily in our IT department) so we can update and patch software flaws.
2. With respect to our relational database, we have three specific safeguards upon which we rely heavily:

a. A person accessing our database must have 'authorization' to enter into the database.

b. A person entering the database must be connecting from a known IP address.

c. All database transactions are monitored and filed thus establishing a 'fingerprint system' by name of all who were inside the database.

3. All SCDMV employees undergo an internal state background investigation prior to offer of employment.
4. We have implemented a 'strong password' system across the agency which mitigates casual use by a fellow employee.

5. SCDMV monitors all outgoing encrypted e-mails via the "Iron port device". This prevents outgoing email to pass Social Security Numbers outside our network and allows SCDMV to examine the profile of all who are using the internal e-mail system to send items out. This is specifically useful if someone wants to send data out of the agency.
6. Per a recommendation from the FBI, we sent all our IT Senior Leaders to a certification class on how to prevent, detect, and respond to Insider IT threats and crimes.

**LLR:**

Changes as a result of the data loss at DHHS & illegal data changes with Cosmo

- The main licensing system has been modified such that any change(s) to SSN, last name or DoB are now tied to a role called "Board Admin". Only authorized personnel have access to change this data.
- All building security has been audited and restricted based on an as needed basis outside of core work hours.
- All emails containing SSN or Credit Card # are encrypted using a method that requires recipients to login to retrieve. This includes attachments to an email.
- All board administrators given real time mechanism to check to see what personnel has rights to their respective board.
- LLR has pending "use" policies that restrict further the access of users to external sites and provide for more monitoring of internet usage.
- VPN account are audited on a quarterly basis. Inactivity over a certain time results in disabled accounts.
- Lastly, we are working on a new mechanism for generating documents that limits and logs all user activity to what is generated to prevent unauthorized documents.

This list was in place prior to the DHHS incident and all remain in place today

- All database permissions are built around the concept of least permissions. All new database objects adhere to this standard.
- Real time database monitors are in place that notify if any suspect access occurs.
- All database backups that contain PI (Personal Information) are encrypted.
- Agency computers have locked USB access. Those requiring USB drives must have a signed request form on record. Form must be authorized by Deputy Director of area.
- Agency laptops use full disk encryption so that in the event the laptop is lost or stolen no one can gain access to the contained agency info.
- LLR just implemented a new firewall with intrusion detection
- As part of the agency's e-commerce compliance, we undergo quarterly vulnerability scans from an independent 3rd party and issues found must be resolved and rescanned.
- Access to websites termed "Cloud Storage" is blocked. These sites allow users to upload files.
- VPN accounts require a signed request form authorized by Deputy Director of area. All communications through the VPN are encrypted.
- No access to/from agency computers using "Go To My PC", etc.
- Ecommerce data is not kept on file like some web sites. Once transaction is complete, the user data is safely removed.

**DJJ:**

This addresses a request from Ted Pitts to provide information regarding efforts by Cabinet Agencies to reinforce information security efforts in light of a recent breach of personally identifiable information (PII) at a state agency.

Anonymity and confidentiality of PII regarding the children entrusted to the care of the SC Department of Juvenile Justice (DJJ) is a part of our legal and moral obligation, as well as a deeply-ingrained value for DJJ staff. Exchange of some of this information is vital and necessary for the law enforcement, judicial, medical, social service and mental health communities, among others, with which DJJ collaborates in order to carry out its responsibilities—both to the citizens of SC and the children entrusted to our care.

This exchange of information now principally is carried out via the Juvenile Justice Management System (JJMS) and the recently-developed Juvenile On-Demand Access (JODA) system. In the two meetings that DJJ had with George Davis, Investigator, from the Office of the Inspector General (IG), it was explained that SCEIS was (is) not a part of the examination regarding information security. That system has well-know protections, and access is controlled to those staff designated to have a business need-to-know.

Similar protections are in place for Juvenile information in the JJMS. Only those staff who must enter, update and use the files for research for the courts or agency-required research are provided access. Information supplied through JODA to law enforcement (whose department signs a memorandum of agreement [MOA] on the use of the system) e.g., name, address, demographic information and photo, as well as arrest record with case disposition is also closely guarded and supplied only to those with which DJJ has executed the MOA.

The IG review identified, in its preliminary response to DJJ, areas that will require additional resources and some considerable time to execute; however, DJJ has taken some interim steps that it believes to be important.

First, Director Barber addressed her Executive Management Team and the Senior Managers at the agency, where she emphasized the need to be careful with PII of our staff, victims and families of children entrusted to DJJ's care—in addition to the children themselves. Training on information security has already been added to new supervisor's training, and is in the process of being included in the week-long new employee orientation for all new DJJ employees. It will also be a part of recurring training events provided to DJJ staff.

DJJ employs a single physical network with users who have varying levels of access determined by userid/password and physical location. Educational Services, Rehabilitative Services, etc. have separate storage areas which can be accessed via the DJJ network. Juvenile Justice Management System (JJMS) is an application that is available on the network. It is also available externally via the Internet to authorized users.

DJJ uses the Symantec Ghost tool to re-image workstations after use (both owned and leased). GDisk disk wipe is a component of the Symantec Ghsot tool that has a secure disk wiping function. GDisk conforms to the U.S. Department of Defense National Industrial Security Program Operating Manual, DoD 5220.22-M.

DJJ employs the Image Overwrite feature on Xerox devices. This feature provides Immediate Image Overwrite (IIO) and On-Demand Image Overwrite (ODIO). IIO means that all temporary files created by a print, copy, or scan job are overwritten when the job is completed. ODIO allows for the overwriting of all temporary files on the devices by request from the operator. As a precautionary safeguard, IT staff is validating that the Image Overwrite feature has been installed and is properly functioning on all Xerox devices.

DJJ has a Working Group, including the Deputy Director for Administrative Services (DDAS), the Information Technology Office Administrator and the Network Administrator (a major function of which is Information Security) to further examine options for improvement of what DJJ believes to be an already very secure information security system.

**DOT:**

- Stopped using Social Security numbers when acquiring data for certain agency functions (example: used to require Social Security number when requesting a parking space – it is no longer required and old files have been purged).
- Eliminated SSN from all reports.
- Added encryption onto files that contain Personally Identifiable Information (PII).
- Implemented SCEIS which deleted use of some of the old systems that held personal data, thereby housing data with DSIT and not the agency(Example: Legacy Procurement system had SSN for certain vendors/consultants as the Federal Identification Number(FEIN). SCEIS replaced the FEIN with a new Vendor Number.
- Implemented strong password policy that requires renewal every 90 days.

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Wednesday, October 24, 2012 6:34 PM
**To:** 'Tim Kelly'
**Subject:** FW: Agency follow up
**Attachments:** Confidentiality Regs-Policies.pdf

**Importance:** High

**Department of Commerce:**

The South Carolina Department of Commerce updated its confidentiality agreement with all of our employees to include social media. In addition, employees will sign a new agreement every year as part of their EPMS process.

In June of 2012, our agency met with an auditor from the Inspector General's Office working on a security project for the Governor's Office. He indicated that Commerce did not maintain personal information and was outside the scope of his current review.

**PPP:**

SCDPPPS has jurisdiction over more than 32,000 criminal offenders who are on probation, parole or other forms of supervision. Records are maintained on all of them, as well data on previous offenders who are no longer under the Department's supervision. Some of the data are public by law (sentences and convictions), and confidential (SSNs, victim and family names).The Department has policies, procedures and software in place to protect the disclosure of the confidential data. The Department is committed to ensuring the integrity and safety of its data and data system by continuously assessing and enhancing its security measures. Some of those protection measures include internal and external systems such as:

Current Internal / External Protocols

- Department personnel may only access the data system upon granting of security level rights. The restricted rights are based on the employee's role and level of responsibility within the Department. Rights are granted through a multi-step approval process involving supervisors and the Department's Strategic Development and Information Technology (SDIT).
- The Department maintains a designated SDIT staff person responsible for monitoring system security. This monitoring includes, but is not limited to: viruses, malware, system breaches, assessment of internal use patterns, etc.
- The Department maintains multiple system monitoring strategies, to include but not limited to: firewalls, networking inspection appliances, network monitoring, and data loss protection systems.

Data Authorization / Control

The Department maintains strict protocols for managing the release of data.

- All data provided in electronic format is encrypted and requires additional security protocols for the user to access.
- The Department maintains written agreements with law enforcement entities for the release of requested data.
- Data released to non-law enforcement entities require a specific request that is reviewed for purpose, data range, etc., prior to being considered for release.
- Department maintains a formal data request process for internal and external customers. Each request is outlined and submitted for review by Divisional Management before being approved. All data requests require the approval of the Director before being approved.

Pending Strategies to Enhance Data Security

- In conjunction with the Governor's strategy to enhance data security, the Department has participated with the Inspector General's Office to conduct a review of its data security system.
- The Department is scheduled to migrate to a Microsoft platform in early 2013 and this will allow for significant security enhancements and the implementation of a two (2) factor authentication model.
- The Department is pending implementation of annual security awareness training for all staff.

**DPS:**

SCDPS - Personal Protection / Securing Data

SCDPS' status as a law enforcement agency requires us to establish clear and explicit standards on appropriate and acceptable uses of our computer resources and information systems.

Because of DPS's law enforcement responsibility, the department's "network" and information systems adhere to standards set forth in the Commission on Accreditation for Law Enforcement Agencies (CALEA). We are inspected (reaccredited) every 3 years.

DPS accepts and maintains CJIS (Criminal Justice Information Systems) Security Policy as the minimum level of security requirements acceptable for the transmission, processing, and storage of the nation's CJIS data.

DPS meets all SLED, CJIS, FBI, NCIC, and NLETS Security and Technical requirements. (Criminal History information.)

DPS has numerous policy Directives in place to address securing data issues: Computer Privacy Policy, Password Security, Information Technology, Appropriate Use of Computer Resources, Network and Information Systems Management, Records Management, and Release of Information Policies.

DPS also issued a "Special Directive/Policy" on the Storing of Sensitive Equipment. Equipment items, especially laptops and vehicle consoles, contain sensitive information. Great care will be taken when the equipment remains in an unattended vehicle used by department personnel in the performance of their duties.

Our Office of Information Technology (OIT) is charged with assuring the integrity of the Department's network and its information systems by utilizing several requirements (Access controls; Utilizes password security systems; Routinely monitors users' accounts; and Audit trail of computer activity, etc.) Additionally, the OIT utilizes several other measures such as:

- SCDPS has a system to alert IT personnel if an intrusion of an unidentified source tries to gain access to our system.
- The computer operating system is automatically locked after 15 minutes without any user activity.
- SCDPS members are prohibited from sharing passwords.
- All access is password protected.
- Access to Human Resource data is largely administered by the State OHR and SCEIS. Very few personnel with SCDPS have access to this data.

**DEW:**

We perform the following functions as part of normal business process to prevent PII data loss:

Network and Data Security --

- All text email sent from the Agency is automatically scanned for PII - specifically data that appears to be SSNs, credit cards.
- Unauthorized email to a large distribution group is automatically restricted.
- Large emails are prevented from being sent outside the Agency until the email is verified by a human to be valid for work use.

- Tools and devices are in place that prevent malicious hacking of our network and web applications and databases
- Laptops used by agents in the field are encrypted in case of loss

Awareness Training --

- All employees are required to take IT security training as part of their onboarding that specifically informs of the proper use and protection of PII.
- All employees are required to read and acknowledge security policies, procedures to include acceptable use of PII

Physical Protection --

- Sensitive areas with PII are accessed by key card only

Actions taken after the DHHS breach:

- All remote access by employees is secured using best practice authentication measures ("two-factor authentication")
- Controls have been implemented to ensure that access to mainframe and other applications is promptly revoked for DEW staff when they terminate employment.
- IT is scanning computers in the SCWorks centers for files containing PII.
- Upgraded the network infrastructure with modern and more secure components (routers, switches).
- Additional security measures and physical controls (sign in log, locked containers) were implemented for the warehouse to increase security over stored paper documents.
- A system configuration issue with the email filter (detecting SSNs) was identified and corrected.
- Hard drives from all computer equipment that will be transferred to State Surplus Property, or disposed of in any other way, are now being removed and destroyed by IT staff prior to the computers being transported to the DEW warehouse.

Because of the Agency re-organization, the following additional steps were taken last week to protect the Agency from possible malicious intent:

- Flagged email that seemed suspicious for affected employees. Follow up to be conducted by IT. Suspicious emails may include those that have large attachments, odd subject lines, or are being sent to outside email addresses (media, etc)
- Audits of application and data access for the affected employees to ensure it was necessary for job duties.

Please let me know if you have any questions.

Joe

**PRT**

1. Removed employee SSN from all HR / personnel paperwork (EPMS, leave forms, etc).

2. When selected vendors for point-of-sale and reservation system required that they be PCI compliant. (We do not capture or store any credit card numbers – all information is encrypted and sent to vendors.)

**SCDHHS:**

Following the Medicaid data breach in April 2012, SCDHHS took several significant steps to alter the way data, including personal health information (PHI) and personally identifiable information (PII) is accessed and managed within the agency.

The following policies and procedures have been updated based on this incident:

DATA ACCESS AND SECURITY POLICIES

Restricted access to data and data warehouse to align access to employee duties (April, 2012)

Limit data access to what employee needs to complete job (April, 2012)

Updated policies for granting access to data and data warehouse (April, 2012)

Added functionality to data warehouse to mask PHI/PII by default (May, 2012)

Delivered new tool for program integrity (internal audit) to sample/audit emails

SYSTEMS CHANGES

Updated email infrastructure (modernized email system, July, 2012)

Changes to email system to encrypt email communications whenever possible (forced and automated, July, 2012)

Updated tools to identify potential PHI/PII in email content/body (July, 2012)

Piloting solution to identify potential PHI/PII in email attachments (in-progress)

TECHNICAL SYSTEMS REVIEW

Engaged external security experts (SECNAP) to deliver technical assessment and recommendations for infrastructure and security (in-progress)

DATA MANAGEMENT PROCESS REVIEW

Engaged external security experts (Gartner) to deliver assessment and recommendations for data, process and system related security, compliance and risk (in-progress)

CRISIS MANAGEMENT PLAN

Completed internal assessment of handling of data release and recommendations for crisis management plan (August 2012)

Implementation of recommendations for crisis management planning and team identification (in-progress)

RELATED PERSONELL POLICIES AND TRAINING

Updated HIPAA Policy — Beginning May 2012, the HIPAA policy has been changed from being a one-time training at hire/orientation to an annual review/update by all employees.

Conflict of Interest/Outside Employment — The agency implemented an Outside Employment Policy and it is now included in the employee orientation. This policy is designed to deter employees from improperly benefitting from their position and/or the data they may have access to at SCDHHS.

**SCDMV:**

SCDMV has taken the following measures to prevent data theft from an internal threat:

1. We disabled USB ports that provide thumb drive access to our computers. That said, we do have a few specific personnel who retain that capability (less than 20 - primarily in our IT department) so we can update and patch software flaws.
2. With respect to our relational database, we have three specific safeguards upon which we rely heavily:
   a. A person accessing our database must have 'authorization' to enter into the database.
   b. A person entering the database must be connecting from a known IP address.
   c. All database transactions are monitored and filed thus establishing a 'fingerprint system' by name of all who were inside the database.
3. All SCDMV employees undergo an internal state background investigation prior to offer of employment.
4. We have implemented a 'strong password' system across the agency which mitigates casual use by a fellow employee.
5. SCDMV monitors all outgoing encrypted e-mails via the "Iron port device". This prevents outgoing email to pass Social Security Numbers outside our network and allows SCDMV to examine the profile of all who are using the internal e-mail system to send items out. This is specifically useful if someone wants to send data out of the agency.
6. Per a recommendation from the FBI, we sent all our IT Senior Leaders to a certification class on how to prevent, detect, and respond to Insider IT threats and crimes.

**LLR:**

Changes as a result of the data loss at DHHS & illegal data changes with Cosmo

- The main licensing system has been modified such that any change(s) to SSN, last name or DoB are now tied to a role called "Board Admin". Only authorized personnel have access to change this data.
- All building security has been audited and restricted based on an as needed basis outside of core work hours.
- All emails containing SSN or Credit Card # are encrypted using a method that requires recipients to login to retrieve. This includes attachments to an email.
- All board administrators given real time mechanism to check to see what personnel has rights to their respective board.
- LLR has pending "use" policies that restrict further the access of users to external sites and provide for more monitoring of internet usage.
- VPN account are audited on a quarterly basis. Inactivity over a certain time results in disabled accounts.
- Lastly, we are working on a new mechanism for generating documents that limits and logs all user activity to what is generated to prevent unauthorized documents.

This list was in place prior to the DHHS incident and all remain in place today

- All database permissions are built around the concept of least permissions. All new database objects adhere to this standard.
- Real time database monitors are in place that notify if any suspect access occurs.
- All database backups that contain PI (Personal Information) are encrypted.
- Agency computers have locked USB access. Those requiring USB drives must have a signed request form on record. Form must be authorized by Deputy Director of area.
- Agency laptops use full disk encryption so that in the event the laptop is lost or stolen no one can gain access to the contained agency info.
- LLR just implemented a new firewall with intrusion detection
- As part of the agency's e-commerce compliance, we undergo quarterly vulnerability scans from an independent 3rd party and issues found must be resolved and rescanned.
- Access to websites termed "Cloud Storage" is blocked. These sites allow users to upload files.
- VPN accounts require a signed request form authorized by Deputy Director of area. All communications through the VPN are encrypted.
- No access to/from agency computers using "Go To My PC", etc.
- Ecommerce data is not kept on file like some web sites. Once transaction is complete, the user data is safely removed.

**DJJ:**

This addresses a request from Ted Pitts to provide information regarding efforts by Cabinet Agencies to reinforce information security efforts in light of a recent breach of personally identifiable information (PII) at a state agency.

Anonymity and confidentiality of PII regarding the children entrusted to the care of the SC Department of Juvenile Justice (DJJ) is a part of our legal and moral obligation, as well as a deeply-ingrained value for DJJ staff. Exchange of some of this information is vital and necessary for the law enforcement, judicial, medical, social service and mental health communities, among others, with which DJJ collaborates in order to carry out its responsibilities—both to the citizens of SC and the children entrusted to our care.

This exchange of information now principally is carried out via the Juvenile Justice Management System (JJMS) and the recently-developed Juvenile On-Demand Access (JODA) system. In the two meetings that DJJ had with George Davis, Investigator, from the Office of the Inspector General (IG), it was explained that SCEIS was (is) not a part of the examination regarding information security. That system has well-know protections, and access is controlled to those staff designated to have a business need-to-know.

Similar protections are in place for Juvenile information in the JJMS. Only those staff who must enter, update and use the files for research for the courts or agency-required research are provided access. Information supplied through JODA to law enforcement (whose department signs a memorandum of agreement [MOA] on

the use of the system) e.g., name, address, demographic information and photo, as well as arrest record with case disposition is also closely guarded and supplied only to those with which DJJ has executed the MOA.

The IG review identified, in its preliminary response to DJJ, areas that will require additional resources and some considerable time to execute; however, DJJ has taken some interim steps that it believes to be important.

First, Director Barber addressed her Executive Management Team and the Senior Managers at the agency, where she emphasized the need to be careful with PII of our staff, victims and families of children entrusted to DJJ's care—in addition to the children themselves. Training on information security has already been added to new supervisor's training, and is in the process of being included in the week-long new employee orientation for all new DJJ employees. It will also be a part of recurring training events provided to DJJ staff.

DJJ employs a single physical network with users who have varying levels of access determined by userid/password and physical location. Educational Services, Rehabilitative Services, etc. have separate storage areas which can be accessed via the DJJ network. Juvenile Justice Management System (JJMS) is an application that is available on the network. It is also available externally via the Internet to authorized users.

DJJ uses the Symantec Ghost tool to re-image workstations after use (both owned and leased). GDisk disk wipe is a component of the Symantec Ghsot tool that has a secure disk wiping function. GDisk conforms to the U.S. Department of Defense National Industrial Security Program Operating Manual, DoD 5220.22-M.

DJJ employs the Image Overwrite feature on Xerox devices. This feature provides Immediate Image Overwrite (IIO) and On-Demand Image Overwrite (ODIO). IIO means that all temporary files created by a print, copy, or scan job are overwritten when the job is completed. ODIO allows for the overwriting of all temporary files on the devices by request from the operator. As a precautionary safeguard, IT staff is validating that the Image Overwrite feature has been installed and is properly functioning on all Xerox devices.

DJJ has a Working Group, including the Deputy Director for Administrative Services (DDAS), the Information Technology Office Administrator and the Network Administrator (a major function of which is Information Security) to further examine options for improvement of what DJJ believes to be an already very secure information security system.

**DOT:**

- Stopped using Social Security numbers when acquiring data for certain agency functions (example: used to require Social Security number when requesting a parking space – it is no longer required and old files have been purged).
- Eliminated SSN from all reports.
- Added encryption onto files that contain Personally Identifiable Information (PII).
- Implemented SCEIS which deleted use of some of the old systems that held personal data, thereby housing data with DSIT and not the agency(Example: Legacy Procurement system had SSN for certain vendors/consultants as the Federal Identification Number(FEIN). SCEIS replaced the FEIN with a new Vendor Number.
- Implemented strong password policy that requires renewal every 90 days.

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Wednesday, October 24, 2012 6:46 PM
**To:** 'tcsmith@greenvillenews.com'
**Subject:** Follow up - quote from our office

Quote from Rob Godfrey, Haley spokesman:

"State government is entrusted with vital personal information from South Carolinians, it's our job to secure that personal information, and that's why the governor asked Inspector General Patrick Maely to review information security at Cabinet agencies and make recommendations for how to strengthen it. Many Cabinet agencies have already strengthened their information security, and we're not going to stop until we have the strongest information security practices in the country."

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Wednesday, October 24, 2012 10:27 PM
**To:** 'Emily.Brady@chernoffnewman.com'
**Cc:** 'Rick.Silver@chernoffnewman.com'; 'Tim.Kelly@chernoffnewman.com'
**Subject:** Re: Experian question

I reached out to Bryan and Ted as soon as I got your message. They will be able to get you an answer on both fronts first thing in the morning. Thanks for following up.

Rob

**From**: Emily Brady [mailto:Emily.Brady@chernoffnewman.com]
**Sent**: Wednesday, October 24, 2012 09:59 PM
**To**: Godfrey, Rob
**Cc**: Rick Silver <Rick.Silver@chernoffnewman.com>; Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Subject**: RE: Experian question

Rob- Have you gotten feedback from Ted/Bryan about Experian? Are they ok with the reasoning for one credit bureau? We are really going to need an answer about moving forward with getting Experian services in place in order to include in our messaging, website, press conference, etc.

Also- is your office reaching out to Consumer Affairs to get them on board? They have a toll-free hotline phone number that we could potentially use if Experian is not in place yet but would need to get them on board. We had discussed having the administrator, Carrie, being at press conference too to explain how consumers can protect themselves.

*Emily Brady*
*Manager of Public Affairs*
*Chernoff Newman*
*1411 Gervais St, 5th Floor*
*Columbia, SC 29201*
*(803) 233-2452*
*Emily.Brady@cnsg.com*
*www.chernoffnewman.com*

---

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Wed 10/24/2012 6:30 PM
**To:** Emily Brady
**Cc:** Rick Silver; Tim Kelly
**Subject:** Re: Experian question

How do y'all want me to handle getting y'all background from state agencies regarding steps take to strengthen information security?

**From**: Emily Brady [mailto:Emily.Brady@chernoffnewman.com]
**Sent**: Wednesday, October 24, 2012 06:27 PM
**To**: Godfrey, Rob
**Cc**: Rick Silver <Rick.Silver@chernoffnewman.com>; Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Subject**: Experian question

Rob-

We have spoken with Experian about the issue of one credit bureau versus three, and based on the the information they shared with us, here is the answer that we have developed. Please share with Bryan and Ted.

Experian is the largest of all of the three credit bureaus and should catch up to 95% of issues. We made the determination that the maginal increase in protection versus the significance in cost was not justified.

Thank you,
Emily

*Emily Brady*
*Manager of Public Affairs*
*Chernoff Newman*
*1411 Gervais St, 5th Floor*
*Columbia, SC 29201*
*(803) 233-2452*
*Emily.Brady@cnsg.com*
*www.chernoffnewman.com*

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Thursday, October 25, 2012 5:02 PM
**To:** Pitts, Ted
**Cc:** LeMoine, Leigh
**Subject:** Fw: Talking points
**Attachments:** Talking points gov.docx

**From**: Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
**Sent**: Wednesday, October 24, 2012 07:33 PM
**To**: Godfrey, Rob
**Subject**: Talking points

See attached suggestions for the governor.

**Gov. Haley Talking Points**

- The State of South Carolina is the victim of a crime committed by a very sophisticated hacker.
- When I learned of this situation, I immediately directed Director Etter and Chief Keel to take all necessary measures to protect the taxpayers, seal the system and identify the perpetrators.
- This requires an unprecedented, large-scale response by the Department of Revenue, the State of South Carolina and all our citizens.
- Among the steps we are taking to protect the taxpayers is providing one year of identity theft protection and credit monitoring to all those who may be affected.
- 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 since 1998.
- 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 instructed the Inspector General to....
- I have confidence that the Department is taking the right steps and that Chief Keel's investigation will not only uncover who did this, but also give us insight into how to better protect ourselves in the future.
- 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.

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Thursday, October 25, 2012 6:24 PM
**To:** 'Tim.Kelly@chernoffnewman.com'
**Subject:** Re: Emailing: DOR.pdf

Great.

----- Original Message -----
From: Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
Sent: Thursday, October 25, 2012 06:21 PM
To: Godfrey, Rob
Subject: Emailing: DOR.pdf

<<DOR.pdf>> Visual for press conference...being produced now.

Your message is ready to be sent with the following file or link attachments:

DOR.pdf

Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

# State of South Carolina

## Executive Department

FILED

OCT 26 2012

Mark Hammond
SECRETARY OF STATE

## Office of the Governor

**EXECUTIVE ORDER NO. 2012-10**

**WHEREAS**, the State's information technology (IT) policy for governance of IT initiatives throughout state government, including security procedures and protocols, has been largely uncoordinated and outdated exposing the State to greater risks of internal and external cyber-attacks on IT infrastructure and records; and

**WHEREAS**, state government's fragmented approach to IT security makes South Carolina vulnerable to serious cyber and information breaches and requires immediate action to minimize cyber-attacks and protect personal information of our State's citizens; and

**WHEREAS**, Section 1-6-30 of the South Carolina Code of Laws authorizes the State Inspector General to "coordinate investigations" and "recommend policies and carry out other activities designed to deter, detect, and eradicate fraud, waste, abuse, mismanagement . . . "; and

**WHEREAS**, Section 1-6-20(E) states, "Upon request of the State Inspector General for information or assistance, all agencies are directed to fully cooperate with and furnish the State Inspector General with all documents, reports, answers, records, accounts, papers, and other necessary data and documentary information to perform the mission of the State Inspector General[;]" and

**WHEREAS**, the State Inspector General is authorized to recommend policies to address holistic mismanagement of state government's information security policies and procedures and state agencies are required to fully cooperate with the State Inspector General to perform his mission.

**NOW, THEREFORE**, I hereby direct all cabinet agencies to immediately designate an information technology officer to cooperate with the State Inspector General who is authorized to make recommendations to improve information security policies and procedures in state agencies, on a comprehensive and holistic basis,

pursuant to his authority under Chapter 6 of Title 1 of the South Carolina Code of Laws with the following additional guidance:

1. Collaborate with the Division of State Information Technology of the Budget and Control Board to identify weaknesses in current statewide cyber-security systems, to include vulnerabilities to internal and external cyber-attacks, and develop a holistic strategy to improve information security;

2. Consult with national cyber-security sources including, but not limited to, the Multi-State Information and Sharing Analysis Center;

3. Determine state agencies' current information security staffing and their specific duties, and work with agencies to identify designated information security officers (ISOs) and their duties at each agency where appropriate; and

4. Improve and increase training of ISOs and all state government employees on information security measures to include cyber-security and records protection.

This Order shall take effect immediately.

**GIVEN UNDER MY HAND AND THE GREAT SEAL OF THE STATE OF SOUTH CAROLINA, THIS 26th DAY OF OCTOBER 2012.**

**NIKKI R. HALEY**
**Governor**

ATTEST:

MARK HAMMOND
SECRETARY OF STATE

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 9:27 AM
**To:** 'Emily Brady'
**Subject:** RE: Press Conference

Has been pushed back.

**From:** Emily Brady [mailto:Emily.Brady@chernoffnewman.com]
**Sent:** Friday, October 26, 2012 9:26 AM
**To:** Godfrey, Rob
**Subject:** Fwd: Press Conference

Are you still meeting with wltx and Greenville news now?

Emily Brady
Manager of Public Affairs
Chernoff Newman
1411 Gervais St, 5th Floor
Columbia, SC 29201
P 803.233.2452
F 803.252.2016
Emily.Brady@cnsg.com
www.chernoffnewman.com

Sent from my iPhone

Begin forwarded message:

> **From:** "Jim Etter" <Etter_JF@sctax.org>
> **Date:** October 26, 2012 9:20:36 AM EDT
> **To:** rush.smith@nelsonmullins.com, Rick.Silver@chernoffnewman.com, Emily.Brady@chernoffnewman.com, Tim.Kelly@chernoffnewman.com, patrickmaley@oig.sc.gov, "Samantha Cheek" <CheekS@sctax.org>, "Harry Cooper" <COOPERH@sctax.org>
> **Cc:** "Ted Pitts" <tedpitts@gov.sc.gov>
> **Subject: Press Conference**
>
> The 11:30 will be delayed. It will happen today but is still in the air.
> I will keep you posted.
>
> Jim Etter
> Director
> SC Department of Revenue
> 803-315-0192

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 12:49 PM
**To:** 'tcsmith@greenvillenews.com'
**Subject:** Re: website, toll free number problems

Just called you.

----- Original Message -----
From: Smith, Tim [mailto:tcsmith@greenvillenews.com]
Sent: Friday, October 26, 2012 12:40 PM
To: Godfrey, Rob
Subject: website, toll free number problems

Rob,

The website for taxpayers to visit requires a login. What do we tell readers? And the toll-free number has a wait. If you are asking millions of taxpayers to visit/call, we need to know how they can get through.

Tim

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 1:02 PM
**To:** Pitts, Ted
**Subject:** Fw:
**Attachments:** 5. Mandiant Overview.pdf; 4. Cabinet Agency Information Security Policy Highlights.docx; 3. Consumer Safety Solutions.docx; 2. Chronology.docx; 1. DOR media release.docx

**From**: Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
**Sent**: Friday, October 26, 2012 07:49 AM
**To**: Godfrey, Rob; Rick Silver <Rick.Silver@chernoffnewman.com>; Jim Etter <Etter_JF@sctax.org>; Harry Cooper <COOPERH@sctax.org>; Samantha Cheek <CheekS@sctax.org>; Liz Mason <MasonL@sctax.org>
**Cc**: Rush Smith <rush.smith@nelsonmullins.com>; jon.neiditz@nelsonmullins.com <jon.neiditz@nelsonmullins.com>; ofonseca@experianinteractive.com <ofonseca@experianinteractive.com>
**Subject**:

Media package contents are attached, including the formatted press release. I'll need any changes to the release by 9:15 am in order to assemble the press kits. If there are no changes to the other documents, I'm going to print those at 8:30 come hell or high water.

Thanks to everyone for your patience and professionalism, two qualities I rarely display myself!

TK

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

1411 Gervais Street
Columbia, SC 29201

- Follow Chernoff Newman

MANDIANT

# Mandiant Overview

**OVERVIEW**

Mandiant is the go-to company for organizations that want to protect their most valuable assets from advanced attack groups including the Advanced Persistent Threat (APT). Our products and services equip you to find and stop advanced attackers before they achieve their objectives. Our engineers and security consultants hold top government security clearances, have written 12 books and are regularly quoted by leading media organizations.

**THE PROBLEM WE SOLVE**

The majority of advanced targeted attacks proceed undetected and proliferate undefended. Simply stated, Mandiant is the only information security company that can tell an organization when it has been compromised and to what extent its defenses have been violated. Mandiant's unique blend of intelligence, expertise and advanced technology prepare you to respond as fast as the attackers no matter how advanced or persistent they are. Our approach --- backed up by our experience on the front lines of advanced attacks --- is why one third of the Fortune 100 rely on Mandiant to detect, respond to and contain targeted attackers.

**CUSTOMERS**

Mandiant's 450+ customers are comprised of a "Who's Who" of the Fortune 1000 including top financial institutions, manufacturers, biotech and technology companies. Highlights include:

- 33% of the Fortune 100
- 70% of the largest defense contractors
- World's largest financial institutions
- The U.S. Department of Defense & federal law enforcement

**WHAT MAKES MANDIANT DIFFERENT**

Our clients are often surprised at the difference before and after engaging Mandiant. In short, with Mandiant you can package up your smartest and most effective incident responders and forensics analysts and scale them to investigate thousands of systems.

**We Help You Triage Alerts & Investigate Incidents Faster and at Scale**: We routinely work in environments with 100,000 endpoints or more. With Mandiant you can sweep thousands of endpoints an hour using our Indicators of Compromise (IOC) while traditional forensics providers would only be able to analyze a few dozen.

**We Use Automated Processes to Create & Share Threat Intelligence**: We have developed tools, processes and techniques to rapidly share threat intelligence, analyze malware and create new intelligence in a machine-readable format. This minimizes the time from when a new threat is identified to when you are able to search for it across every system in your environment.

**We Know What to Look For**: Our products and services are directed by the latest intelligence from the front lines. If we've seen it before (and we've seen a lot) we capture it in our Indicators of Compromise library so you'll be able to search for the same threats across your organization.

**We See What Others Can't**: With visibility into both your endpoints and your network, we find evidence of compromise that goes well beyond malware. Our intelligence and tools enable you to find where the attacker has been and what they've accessed.

**We're Experts At What We Do**: We're on the front lines every day but we can't be everywhere. That's why we created products that put the same tools and intelligence in your hands that our consultants use in the field every day.

**"With Mandiant, we believe we can determine the scope of an attack so that we can respond faster, limit losses and minimize the disruption to our ongoing business."**

- Global Security Architect, Aerospace Manufacturer

# Mandiant Overview

**PRODUCTS**

Whether you are looking to equip your own incident response team or hire Mandiant to assess your environment and protect you from advanced threats, our products have you covered. Our two major product offerings include:

- **Mandiant Intelligent Response®:** Today's threat actors are savvy, sophisticated, and relentless. They target human vulnerabilities to slip through your preventive defenses. When they do, Mandiant Intelligent Response (MIR®) enables you to hunt for advanced attackers in your environment by scaling your security team and forensics experts to investigate thousands of endpoints, scope an incident and contain the threat.
- **MCIRT™ Managed Defense:** The MCIRT Managed Defense is a full service offering that brings together all of the experts, experience and technology required to find attackers at any stage of the attack and respond aggressively before they complete their mission. Whether it's a spear phishing e-mail, command and control activity or attackers logging into your VPN with stolen user credentials we'll tell you. And we do more than just alert you. We give you context, tell you how to respond and where threats belong on your priority list.

**PROFESSIONAL SERVICES**

Mandiant offers a full portfolio of professional services to train and equip you to identify, investigate and respond to advanced attackers. Our major service offerings include:

- **Incident Response:** Incident response is Mandiant's primary focus and expertise. We have performed hundreds of computer security investigations across all industries, organization sizes and technical environments. We'll tell you who's behind the attack (organized crime, nation state or malicious insider), how much damage was done, and work with you to recover from the incident while minimizing the impact of the event on the organization.
- **Security Program Development:** Do you need help scaling your own incident response (IR) and forensics team? Our IR program development services draw on our own automated processes and experience responding to some of the most complex and high-profile security breaches. We'll benchmark your incident response team against leading practices and help you determine where your program needs to go — and how you can get there.
- **Litigation Support & Forensics:** Mandiant supports organizations facing the prospect of legal action when the interpretation of electronic evidence is required. This can involve supporting its clients in court, protecting them from potential litigation or providing analysis that can be used during internal inquiries.
- **Threat & Vulnerability Assessments:** While many security consulting organizations look for theoretical vulnerabilities, Mandiant works with its clients to assess the strength of their defenses against the tactics that are most likely to be used by actual attackers. Mandiant offers a complete portfolio of threat and vulnerability assessment services that allow organizations to determine when they are already compromised and identify critical security vulnerabilities that attackers could exploit.

**PARTNERS**

We recognize that every good security program includes products and services from many different vendors. With that in mind, Mandiant has developed an extensive network of partners to enhance the value and accelerate the delivery of our solutions. We work hand-in-hand with some of the most respected technology vendors, audit firms and regional channel partners to define the requirements for our products and better serve our global customer base.

**"By knowing what indicators to look for and having the ability to search our entire network in a matter of hours we are able to shrink our window of exposure when threats evade our preventive measures."**

– Chief Information Security Officer, Fortune 500 Financial Services Company

MANDIANT®

Mandiant's products and services protect the world's most valuable data every day from targeted attacks. Our unique combination of intelligence, experience and technology equip organizations to detect, respond and contain attackers before they reach their objective.

TEL +1 (703) 683-3141 TOLL FREE (800) 647-7020 WASHINGTON NEW YORK LOS ANGELES SAN FRANCISCO WWW.MANDIANT.COM

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 2:03 PM
**To:** 'CheekS@sctax.org'
**Cc:** 'ncaula@postandcourier.com'
**Subject:** Re: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Please make sure Natalie Caula ncaula@postandcourier.com is in receipt of the press kit ASAP.

**From**: Samantha Cheek [mailto:CheekS@sctax.org]
**Sent**: Friday, October 26, 2012 02:00 PM
**To**: Samantha Cheek <CheekS@sctax.org>
**Subject**: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

**For Immediate Release: October 26, 2012**

# SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

*Hacker illegally obtained credit card and Social Security numbers*

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

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

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have 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."

###

**Godfrey, Rob**

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:06 PM
**Subject:** S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
**Attachments:** Media_Release_10262012.pdf

# 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**

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:09 PM
**To:** 'Cohen, Keven'
**Subject:** RE: from Keven Cohen

Keven,

Thanks for reaching out. It's always good to hear from you. We are in the process of making sure that you and every media outlet in the state have all of the information you'll need to pass along to your listeners/readers. As we continue to work through that process, I will get with the governor's scheduler to see if the governor has flexibility in the schedule this afternoon – but I'm not sure she does right now.

Again, thanks for reaching out.

Rob

---

**From:** Cohen, Keven [mailto:kev@wvoc.com]
**Sent:** Friday, October 26, 2012 3:06 PM
**To:** Godfrey, Rob
**Subject:** from Keven Cohen

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

Thanks,

Keven

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:31 PM
**To:** 'CheekS@sctax.org'
**Subject:** Re: press inquiry re cyber attack

thanks for handling.

**From**: Samantha Cheek [mailto:CheekS@sctax.org]
**Sent**: Friday, October 26, 2012 03:30 PM
**To**: Ballard, Andrew <aballard@bna.com>; Godfrey, Rob
**Subject**: RE: press inquiry re cyber attack

Andrew,

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

Regards,

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

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

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

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

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

Thanks for your time!

**Andrew M. Ballard**
Staff Correspondent
Raleigh, NC

**BNA, Inc.**

Direct 919.841.1240
aballard@bna.com

more information about BNA is available at http://www.bna.com

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:41 PM
**To:** 'cheeks@sctax.org' (cheeks@sctax.org)
**Subject:** FW: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Can you get this one handled?

---

**From:** GMoore@wspa.com [mailto:GMoore@wspa.com]
**Sent:** Friday, October 26, 2012 3:40 PM
**To:** Godfrey, Rob
**Cc:** CheekS@sctax.org
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hey Rob and Samantha -
So, I just visited protectmyid.com/scdor -- and I'm stumped. If I am, I know our viewers will be. It says enter an activation code, but one is not provided. Can you provide further? To even try to create an account, you need one of these activation codes. Any clue?
Thanks,
Graeme Moore
WSPA-TV
864-809-1806

---

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

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

*Hacker illegally obtained credit card and Social Security numbers*

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

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

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

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

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

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

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

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

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

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

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

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

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

-###-

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:53 PM
**To:** 'Jonathan Allen'
**Cc:** 'shawn@patch.com' (shawn@patch.com)
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

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

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

Rob,

Thank you for sending this information along.

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

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

Thanks,

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

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

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

*Hacker illegally obtained credit card and Social Security numbers*

**COLUMBIA, S.C.** – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in

a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

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

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

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

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

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

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

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

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

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

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

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

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

-###-

**Rob Godfrey**
**Office of Gov. Nikki Haley**

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:53 PM
**To:** 'Harriet McLeod'
**Subject:** RE: Rob, is there a video coming or quotes from the Governor?

Yes.

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

Thanks,
Harriet

--
Harriet McLeod
Reuters America
www.reuters.com

Charleston, South Carolina
843-270-4619 (mobile)
[redacted]@gmail.com

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 3:55 PM
**To:** 'Samantha Cheek'
**Subject:** RE: For Tim Smith at the Greenville News

Call me. Cell phone.

**From:** Samantha Cheek [mailto:CheekS@sctax.org]
**Sent:** Friday, October 26, 2012 3:55 PM
**To:** Godfrey, Rob
**Subject:** RE: For Tim Smith at the Greenville News

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

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

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

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

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:05 PM
**To:** 'Samantha Cheek'
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

What is your cell?

**From:** Samantha Cheek [mailto:CheekS@sctax.org]
**Sent:** Friday, October 26, 2012 3:59 PM
**To:** GMoore@wspa.com; Godfrey, Rob
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Graeme,

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

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

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

Hey Rob and Samantha -
So, I just visited protectmyid.com/scdor -- and I'm stumped. If I am, I know our viewers will be. It says enter an activation code, but one is not provided. Can you provide further? To even try to create an account, you need one of these activation codes. Any clue?
Thanks,
Graeme Moore
WSPA-TV
864-809-1806

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

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

*Hacker illegally obtained credit card and Social Security numbers*

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

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

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

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

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

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

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

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

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

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

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

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

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

-###-

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:05 PM
**To:** 'cheeks@sctax.org' (cheeks@sctax.org)
**Subject:** FW: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
**Attachments:** Media_Release_10262012.pdf; ATT00001.htm

**From:** Gatson, Judi [mailto:jgatson@wistv.com]
**Sent:** Friday, October 26, 2012 3:24 PM
**To:** Godfrey, Rob
**Subject:** Fwd: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Rob,

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

~ jg

Begin forwarded message:

> **From:** "Turner, Michael" <mturner@wistv.com>
> **To:** "All WIS Producers" <AllWISProducers@wistv.com>
> **Subject: FW: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers**
>
> From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
> Sent: Friday, October 26, 2012 3:06 PM
> Subject: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
>
> S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
> Hacker illegally obtained credit card and Social Security numbers
>
> COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.
>
> ***Press kit attached with information regarding the chronology of the investigation and

consumer safety solutions is attached.***

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

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

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

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

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

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

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

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

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

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

"From the first moment we learned of this, our top priority has been to protect the taxpayers and the citizens of South Carolina, and every action we've taken has been consistent with that

priority," Etter said. "We have an obligation to protect the personal information entrusted to us, and we are redoubling our efforts to meet that obligation."
-###-

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:16 PM
**To:** 'Samantha Cheek'
**Subject:** RE: Number info - from SCDOR

Call me.

**From:** Samantha Cheek [mailto:CheekS@sctax.org]
**Sent:** Friday, October 26, 2012 4:16 PM
**To:** Gatson, Judi
**Cc:** Norman, Meaghan; Godfrey, Rob
**Subject:** RE: Number info - from SCDOR

We're unsure as to those details – the call center is open and available for taxpayers to call 24/7.

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

**From:** Gatson, Judi [mailto:jgatson@wistv.com]
**Sent:** Friday, October 26, 2012 3:31 PM
**To:** Samantha Cheek
**Cc:** Norman, Meaghan
**Subject:** Fwd: Number info - from SCDOR

Samantha,

How many operators are currently working that phone line? How many operators do you hope to add? Where is the call center located? And Is the line open 24 hours a day?

Many thx,
~ jg

Begin forwarded message:

> **From:** "Beeker, LaDonna" <lbeeker@wistv.com>
> **Date:** October 26, 2012, 3:29:25 PM EDT
> **To:** All WIS Producers <AllWISProducers@wistv.com>
> **Subject: Number info - from SCDOR**
>
> Just got this ...
>
> **From:** Samantha Cheek [mailto:CheekS@sctax.org]
> **Sent:** Friday, October 26, 2012 3:29 PM
> **To:** Beeker, LaDonna
> **Subject:** RE: Public contact info

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

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

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

Hi Samantha,

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

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

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:19 PM
**To:** 'cheeks@sctax.org' (cheeks@sctax.org)
**Subject:** FW: Mandiant

**From:** Phillips, Noelle [mailto:nophillips@thestate.com]
**Sent:** Friday, October 26, 2012 3:25 PM
**To:** Godfrey, Rob
**Subject:** Mandiant

Hey Rob,

What is the name and title of the Mandiat rep who spoke at today's press conference? Thanks.

--
Noelle Phillips
Reporter
The State Media Co.
(803) 771-8307

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:26 PM
**To:** 'Caula, Natalie'
**Subject:** RE: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Available at governor.sc.gov

**From:** Caula, Natalie [mailto:ncaula@postandcourier.com]
**Sent:** Friday, October 26, 2012 4:23 PM
**To:** Godfrey, Rob
**Subject:** RE: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Thanks Rob. Also, Governor Haley mentioned an executive order during the press conference. Do you have any information on that for release?

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Friday, October 26, 2012 2:03 PM
**To:** Caula, Natalie
**Subject:** Fw: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

**From**: Samantha Cheek [mailto:CheekS@sctax.org]
**Sent**: Friday, October 26, 2012 02:00 PM
**To**: Samantha Cheek <CheekS@sctax.org>
**Subject**: SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

**For Immediate Release: October 26, 2012**

# SC Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

*Hacker illegally obtained credit card and Social Security numbers*

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

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

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have 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."

###

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:26 PM
**To:** Caula, Natalie (ncaula@postandcourier.com)
**Subject:** FW: Executive Order 2012-10 and Letter to Maley
**Attachments:** 2012-10 Reviewing IT Security.PDF; Letter to Maley re EO 2012-10.PDF

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Attachments:** Media_Release_10262012.pdf

**Importance:** High

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**

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:31 PM
**To:** '[redacted]@gmail.com' ([redacted]@gmail.com); 'robbieb@nytimes.com' (robbieb@nytimes.com)
**Subject:** FW: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Attachments:** Media_Release_10262012.pdf

**Importance:** High

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:38 PM
**To:** 'Ashley Byrd'
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

The call center is up.

**From:** Ashley Byrd [mailto:abyrd@southcarolinaradionetwork.com]
**Sent:** Friday, October 26, 2012 4:37 PM
**To:** Godfrey, Rob
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Rob, the call center is not up

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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**

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:44 PM
**To:** 'Shane Massey'
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Sen. Massey,

The first step is to call the call center. There, you'll be provided with an activation code. Here are the steps to take:
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.

Let me know if you need anything else.

Rob

**From:** Shane Massey [mailto:asmlaw30@bellsouth.net]
**Sent:** Friday, October 26, 2012 4:39 PM
**To:** Godfrey, Rob
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Rob,

To do the online protection, you need an activation code. Any idea what that is?

Shane Massey

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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**

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 5:35 PM
**To:** 'cheeks@sctax.org' (cheeks@sctax.org)
**Subject:** FW: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

**From:** Taillon, Jeff
**Sent:** Friday, October 26, 2012 5:35 PM
**To:** Godfrey, Rob
**Subject:** FW: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

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

**From:** McQuary, Anne [mailto:amcquary@WLTX.GANNETT.COM]
**Sent:** Friday, October 26, 2012 5:00 PM
**To:** Taillon, Jeff
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Jeff,

So still just the one number? Do we know if they are adding operators to handle the call volume? Have we asked them if they can go 24/7 to handle the volume?? Hearing from folks that you can add family members once you are online, another caller said you can't. So if you get through, can you do yourself and other family members. What about children who have SS#' can they be added?

Thanks

Anne

**From:** Taillon, Jeff [mailto:JeffTaillon@gov.sc.gov]
**Sent:** Friday, October 26, 2012 4:32 PM
**To:** McQuary, Anne
**Subject:** FW: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

Anne,

I think this should help answer your questions. If there is anything else that I can do for you to be of service please let me know.

Jeff

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

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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**

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 5:36 PM
**To:** 'cheeks@sctax.org' (cheeks@sctax.org)
**Subject:** Call me

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:00 PM
**To:** 'Ashley Byrd'
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

We have increased and are continuing to increase the number of people assisting South Carolinians who call the call center.

**From:** Ashley Byrd [mailto:abyrd@southcarolinaradionetwork.com]
**Sent:** Friday, October 26, 2012 4:37 PM
**To:** Godfrey, Rob
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Rob, the call center is not up

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:00 PM
**To:** 'Shane Massey'
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

We have increased and are continuing to increase the number of people assisting South Carolinians who call the call center.

**From:** Shane Massey [mailto:asmlaw30@bellsouth.net]
**Sent:** Friday, October 26, 2012 4:39 PM
**To:** Godfrey, Rob
**Subject:** RE: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions

Rob,

To do the online protection, you need an activation code. Any idea what that is?

Shane Massey

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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**

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:00 PM
**To:** 'Jonathan Allen'
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

We have increased and are continuing to increase the number of people assisting South Carolinians who call the call center.

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

Rob,

Thank you for sending this information along.

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

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

Thanks,

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

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

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

*Hacker illegally obtained credit card and Social Security numbers*

**COLUMBIA, S.C.** – The South Carolina Department of Revenue today announced that approximately

3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

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

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

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

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

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

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

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

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

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

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

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

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

-###-

**Rob Godfrey**
**Office of Gov. Nikki Haley**

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:00 PM
**To:** 'GMoore@wspa.com'
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

We have increased and are continuing to increase the number of people assisting South Carolinians who call the call center.

**From:** GMoore@wspa.com [mailto:GMoore@wspa.com]
**Sent:** Friday, October 26, 2012 3:40 PM
**To:** Godfrey, Rob
**Cc:** CheekS@sctax.org
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Hey Rob and Samantha -
So, I just visited protectmyid.com/scdor -- and I'm stumped. If I am, I know our viewers will be. It says enter an activation code, but one is not provided. Can you provide further? To even try to create an account, you need one of these activation codes. Any clue?
Thanks,
Graeme Moore
WSPA-TV
864-809-1806

---

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

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

*Hacker illegally obtained credit card and Social Security numbers*

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

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

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

"On October 10, the S.C. Division of Information Technology informed the S.C. Department of Revenue of a potential cyber attack involving the personal information of taxpayers," said DOR Director James Etter. "We worked with them throughout that day to determine what may have happened and what steps to take to

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

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

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

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

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

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

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

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

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

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

-###-

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:00 PM
**To:** 'Phillips, Noelle'
**Subject:** RE: Mandiant

We have increased and are continuing to increase the number of people assisting South Carolinians who call the call center.

**From:** Phillips, Noelle [mailto:nophillips@thestate.com]
**Sent:** Friday, October 26, 2012 3:25 PM
**To:** Godfrey, Rob
**Subject:** Mandiant

Hey Rob,

What is the name and title of the Mandiat rep who spoke at today's press conference? Thanks.

--
Noelle Phillips
Reporter
The State Media Co.
(803) 771-8307

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:01 PM
**To:** 'Gatson, Judi'
**Subject:** RE: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

We have increased and are continuing to increase the number of people assisting South Carolinians who call the call center.

**From:** Gatson, Judi [mailto:jgatson@wistv.com]
**Sent:** Friday, October 26, 2012 3:24 PM
**To:** Godfrey, Rob
**Subject:** Fwd: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers

Rob,

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

~ jg

Begin forwarded message:

> **From:** "Turner, Michael" <mturner@wistv.com>
> **To:** "All WIS Producers" <AllWISProducers@wistv.com>
> **Subject: FW: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers**
>
> From: Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
> Sent: Friday, October 26, 2012 3:06 PM
> Subject: S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
>
> S.C. Department of Revenue Responds to Cyber Attack, Will Provide Credit Monitoring and Identity Theft Protection to Taxpayers
> Hacker illegally obtained credit card and Social Security numbers
>
> COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers have been exposed in a cyber attack. Of the credit cards, the vast majority are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders. Approximately 16,000 are unencrypted.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:01 PM
**To:** 'ellism@independentmail.com'
**Subject:** FW: UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Attachments:** Media_Release_10262012.pdf

**Importance:** High

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 4:28 PM
**Subject:** UPDATE - Video: Gov. Nikki Haley, SLED, U.S. Secret Service, S.C. DOR respond to cyber attack with consumer safety solutions
**Importance:** High

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

**Godfrey, Rob**

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:12 PM
**To:** 'Mary Henry'
**Subject:** RE: Activation Code

**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.

**From:** Mary Henry [mailto:marybhenry@gmail.com]
**Sent:** Friday, October 26, 2012 3:16 PM
**To:** Godfrey, Rob
**Subject:** Activation Code

Rob,

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

How can we get a code?

Mary

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 6:21 PM
**To:** Haltiwanger, Katherine
**Subject:** Constituent call

Sharon Bailey
864 [redacted]

Needs a call back.

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 9:49 PM
**To:** 'tcsmith@greenvillenews.com'
**Subject:** Re: PRESS RELEASE: Nikki Haley, yet again, proves she is more interested in helping her political career than helping South Carolina

First of all, off the record, you and I both know, Tim, that experts, including the one from Mandiant standing with SLED and the Secret Service today, concede there is nothing to Harpootlian's criticism because, as Mandiant's guy said, there are two kinds of businesses: those which have been hacked and those which will be hacked.

Second, on the record, for attribution to Rob Godfrey, Haley spokesman:

"Just because Dick Harpootlian decided it was appropriate to try and turn a criminal attack on South Carolina into a partisan political issue doesn't mean we'll respond in kind. Our focus will remain on making sure the people of our state have the protection they deserve."

----- Original Message -----
From: Smith, Tim [mailto:tcsmith@greenvillenews.com]
Sent: Friday, October 26, 2012 09:31 PM
To: Godfrey, Rob
Subject: FW: PRESS RELEASE: Nikki Haley, yet again, proves she is more interested in helping her political career than helping South Carolina

Rob,

Any response to Harpootlian's stuff, especially the last graf?

Tim

---

From: [redacted]@gmail.com [[redacted]@gmail.com] On Behalf Of Amanda Loveday [aloveday@scdp.org]
Sent: Friday, October 26, 2012 3:59 PM
To: Amanda Loveday
Subject: PRESS RELEASE: Nikki Haley, yet again, proves she is more interested in helping her political career than helping South Carolina

Immediate Release

Press Contact:
Amanda Loveday
803-315-5837
aloveday@scdp.org<mailto:aloveday@scdp.org>

Nikki Haley, yet again, proves she is more interested in helping her political career than helping South Carolina

South Carolina Democratic Party Chairman, Dick Harpootlian, released the following statement in response to the personal information hacked from the Department of Revenue:

Nikki Haley today contradicted the Nikki Haley of yesterday – or maybe came down with a case of Romnesia, which I've heard is contagious.

Haley surrounded herself with federal officials today while telling the people of South Carolina that more than a third of the state's social security numbers and credit card numbers were stolen from her Department of Revenue by a computer hacker. This is a different story than the past year where we've heard Haley stomp her feet and shout that the federal government has no place in our state when it came to the Voter ID law, Medicaid and education funding.

Just two months ago, Haley said in her National Convention speech, "The hardest part of my job continues to be this federal government."

Maybe if she spent more time doing her job in South Carolina rather than traveling around the country raising money and playing politics, someone would have been paying attention and not let more than a third of our state's personal information be compromised.

If she were the CEO of a company that had a third of its data hacked especially after all the public warnings of the danger of hackers, she would be fired. Too bad she has two more years on her contract.

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Friday, October 26, 2012 11:10 PM
**To:** 'Greg.Young@experianinteractive.com'; Stirling, Bryan
**Cc:** 'Ken.Chaplin@experianinteractive.com'
**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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 10:32 AM
**To:** 'CheekS@sctax.org'
**Cc:** Taillon, Jeff
**Subject:** Fw: Follow up on SC Cyber Attack

Samantha,

Good morning. Please follow up with this reporter and email him answers to his questions.

Confirm when this is finished.

Let me know how you're doing today.

Rob

**From**: Fraendy Clervaud [mailto:fclervaud@wach.com]
**Sent**: Saturday, October 27, 2012 10:24 AM
**To**: Taillon, Jeff
**Cc**: Godfrey, Rob
**Subject**: Follow up on SC Cyber Attack

Hey Jeff,
Per our conversation this morning I would like to interview someone on-camera today regarding the SC cyber attack. Anyone from the governor's office, SLED, SC Dept of Revenue would be fine. Here are some of the questions:

1. Any new information on the number of people affected?
2. Phone lines yesterday were extremely busy. Are there new numbers to call? Are there more customer service reps?
3. Any word on WHEN they'll have an idea exactly whose information was compromised?
4. Explain the $1 million id theft insurance policy?
5. Has there been any complaints from SC residents about accounts, credit cards, loans being opened in their names?

Thanks again Jeff. Btw I wanted to know if I could have these questions answered or an interview set up by 3pm today. Let me know.

**Fraendy Clervaud**
Anchor/Reporter
Good Day Columbia
1400 Pickens Street
Columbia SC, 29201
803-609-0269 (Cell)
803-252-6397 (Newsroom)
www.midlandsconnect.com

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 2:12 PM
**To:** 'dcourrege@postandcourier.com'
**Cc:** 'CheekS@sctax.org'
**Subject:** Follow up

Diette --

Good to talk to you. Samantha Cheek or Director Jim Etter at the Department of Revenue should be able to walk you through the answers to your questions. Let me know if you need any answers from our office, such as any you have about timing, but please also watch the full press conference and media avail beforehand at http://www.youtube.com/nikkihaley

Thanks.

Rob

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 2:15 PM
**To:** 'dcourrege@postandcourier.com'
**Cc:** 'CheekS@sctax.org'
**Subject:** More follow up

Diette --

Below you will find information for your story from the second eblast our office provided reporters statewide yesterday afternoon.

Additionally, please visit http://governor.sc.gov to download the full press kit released yesterday, including a chronology of the events leading up to yesterday's announcement.

Thanks.

Rob

---

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

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 2:39 PM
**To:** 'Etter_JF@sctax.org'
**Subject:** Fw: Follow up

Diette Courrage, The Post and Courier 8439375546

----- Original Message -----
From: Godfrey, Rob
Sent: Saturday, October 27, 2012 02:12 PM
To: 'dcourrege@postandcourier.com' <dcourrege@postandcourier.com>
Cc: 'CheekS@sctax.org' <CheekS@sctax.org>
Subject: Follow up

Diette --

Good to talk to you. Samantha Cheek or Director Jim Etter at the Department of Revenue should be able to walk you through the answers to your questions. Let me know if you need any answers from our office, such as any you have about timing, but please also watch the full press conference and media avail beforehand at http://www.youtube.com/nikkihaley

Thanks.

Rob

## Godfrey, Rob

**From:** Godfrey, Rob
**Sent:** Saturday, October 27, 2012 2:39 PM
**To:** 'Etter_JF@sctax.org'
**Subject:** Fw: More follow up

Diette Courrage, The Post and Courier, 8439375546

----- Original Message -----
From: Godfrey, Rob
Sent: Saturday, October 27, 2012 02:15 PM
To: 'dcourrege@postandcourier.com' <dcourrege@postandcourier.com>
Cc: 'CheekS@sctax.org' <CheekS@sctax.org>
Subject: More follow up

Diette --

Below you will find information for your story from the second eblast our office provided reporters statewide yesterday afternoon.

Additionally, please visit http://governor.sc.gov to download the full press kit released yesterday, including a chronology of the events leading up to yesterday's announcement.

Thanks.

Rob

---

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