## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 2:22 PM
**To:** Godfrey, Rob; Stirling, Bryan
**Subject:** FW: Status Update - Review of Information Security at the Cabinet Agencies
**Attachments:** Summary Letter to Governor_Agcy_Data_Sec.docx

**From:** Maley, Patrick
**Sent:** Wednesday, October 24, 2012 1:37 PM
**To:** Pitts, Ted
**Subject:** FW: Status Update - Review of Information Security at the Cabinet Agencies

Attached letter is a status update of project, dated 9/18/12, which simply states methodology & results, which demonstrates due diligence by the Executive Branch in response to DHHS PII incident.

We have DDS and SLED still hanging. Closing loop with DDS is in near term because they should be nearing completion of their survey instrument. SLED just hired an IT Director and I extended their survey completion until after their IT Director can assess their IT system and accurately complete our survey.

I have had media inquiry from Tim Smith, Greenville on this project. I am generally aware of DOR issue. DOR was the only agency we looked that met expectations for having sound information security practices in all nine categories. Further, DOR has to pass requirements & testing to meet Federal IRS standards due to tax data in its custody.

Having sound IT security practices is not a guarantee of not being hacked—it is due diligence to manage the risk.

Call if you need further.

Thanks

**From:** Maley, Patrick
**Sent:** Tuesday, September 18, 2012 3:52 PM
**To:** Pitts, Ted
**Subject:** Status Update - Review of Information Security at the Cabinet Agencies

Ted, attached is a letter I will be sending to the Governor through your office. It is a 2 page, light read, summary of the information security review to date, with expected completion in early October 2012. I am sending this because I sense an upcoming cabinet meeting, and this is a corporate issue impacting the entire cabinet with a very positive, but room to improve, outcome.

I have met about half of the cabinet Agency Directors, and they all have been very gracious and helpful. If you could work me in for a minute or two at the next cabinet meeting, I would like to meet them all as a group and brief them on our course change and continue to seek input before I finalize the OIG tangible objectives.

I will have my final draft objectives in a couple of weeks, and will be circulating for input & you will be on the list.

My new cell is 429-4946.

thanks

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 2:25 PM
**To:** Godfrey, Rob
**Subject:** FW: Confidentiality - PHI Info DOADOS

---

**From:** Roberson, Lillian
**Sent:** Wednesday, October 24, 2012 2:20 PM
**To:** Pitts, Ted
**Cc:** Toomey, Bob; Dutton, Lee
**Subject:** Confidentiality - PHI Info

Ted,

Lee Dutton asked that I forward the information below regarding how alcohol and drug treatment records are secured. Additionally, access to PHI is restricted to only six staff members, and we will be issuing encrypted thumb drives to ensure client information is protected.

Lillian

Confidentiality Regs-Policies....

*Lillian Roberson*
*Manager, Division of Operations*
*S.C. Department of Alcohol and Other Drug Abuse Services*
*PHYSICAL ADDRESS: 2414 Bull Street, Columbia, SC 29201*
*MAILING ADDRESS: PO Box 8268, Columbia, SC 29202*
*phone: 803-896-1145*
*fax: 803-896-5557*

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 2:26 PM
**To:** Godfrey, Rob
**Subject:** FW: Info from SCDHHS
**Attachments:** dhhs-datarelease-update-20121022.docx

**Importance:** High

**From:** Jeff Stensland [mailto:stensland@scdhhs.gov]
**Sent:** Wednesday, October 24, 2012 1:33 PM
**To:** Pitts, Ted
**Cc:** Anthony Keck
**Subject:** Info from SCDHHS
**Importance:** High

Hi Ted,
Attached is the information you requested. Let us know if you need more details.

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:10 PM
**To:** Godfrey, Rob
**Subject:** Fw: Info from SCDHHS

**From**: Anthony Keck [mailto:KECK@scdhhs.gov]
**Sent**: Wednesday, October 24, 2012 03:15 PM
**To**: Jeff Stensland <stensland@scdhhs.gov>; Pitts, Ted
**Cc**: John Supra <SUPRA@scdhhs.gov>
**Subject**: Re: Info from SCDHHS

Nice job. Thanks.

---

**From:** Jeff Stensland
**Sent:** Wednesday, October 24, 2012 1:33:03 PM
**To:** tedpitts@gov.sc.gov
**Cc:** Anthony Keck
**Subject:** Info from SCDHHS

Hi Ted,
Attached is the information you requested. Let us know if you need more details.

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:11 PM
**To:** Godfrey, Rob
**Subject:** Fw: SCDPPPS Data Security

----- Original Message -----
From: Kela Thomas [mailto:kthomas@ppp.state.sc.us]
Sent: Wednesday, October 24, 2012 03:12 PM
To: Scott Norton <SNorton@ppp.state.sc.us>
Cc: Pitts, Ted; Jodi Gallman <JGallman@ppp.state.sc.us>; Peter O'Boyle <POboyle@ppp.state.sc.us>
Subject: Re: SCDPPPS Data Security

Thanks guys, I appreciate your timely response. Ted, I hope this helps.

Sent from my iPad

On Oct 24, 2012, at 2:58 PM, "Scott Norton" <SNorton@ppp.state.sc.us>
wrote:

> Ted,
>
> Attached is an overview of our security protocols. Please let me know
if you have any questions.
>
> Scott Norton
> 803-667-2174
> <SCDPPPS Data security.doc>

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:11 PM
**To:** Godfrey, Rob
**Subject:** Fw:
**Attachments:** SCDPS - Personal Protection Securing Data.docx

**From**: Brooks, Bonnie [mailto:BonnieBrooks@SCDPS.GOV]
**Sent**: Wednesday, October 24, 2012 03:09 PM
**To**: Pitts, Ted
**Cc**: Smith, Leroy <Smith_Leroy@scdps.net>
**Subject**:

Mr. Pitts, Director Smith asked that I forward the attached report to you. Please let him know if you have any questions or need additional information. Thank you.

*Bonnie Brooks*
*Office of the Director*
*S.C. Department of Public Safety*
*10311 Wilson Boulevard (or P.O. Box 1993)*
*Blythewood, S.C. 29016*
*803-896-7979 (Office)*
*803-606-4080 (Cell)*
*803-896-7881 (Fax)*
BonnieBrooks@scdps.gov
www.scdps.gov

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:11 PM
**To:** Godfrey, Rob
**Subject:** Fw: SCDPPPS Data Security
**Attachments:** SCDPPPS Data security.doc

**From**: Scott Norton [mailto:SNorton@ppp.state.sc.us]
**Sent**: Wednesday, October 24, 2012 02:58 PM
**To**: Pitts, Ted
**Cc**: Jodi Gallman <JGallman@ppp.state.sc.us>; Kela Thomas <KThomas@ppp.state.sc.us>; Peter O'Boyle <POboyle@ppp.state.sc.us>
**Subject**: SCDPPPS Data Security

Ted,

Attached is an overview of our security protocols. Please let me know if you have any questions.

Scott Norton
803-667-2174

**Godfrey, Rob**

| | |
|---|---|
| **From:** | Pitts, Ted |
| **Sent:** | Thursday, October 25, 2012 8:36 AM |
| **To:** | Godfrey, Rob |
| **Subject:** | FW: SCDC Information Security |
| **Attachments:** | Security of Personal Information.pdf; DRAFT ADM-15-05.pdf; OIG Evaluation of Cabinet Agencies' Data Security.pdf |

**From:** Trevis Shealy [mailto:Shealy.Trevis@doc.sc.gov]
**Sent:** Wednesday, October 24, 2012 6:19 PM
**To:** Pitts, Ted
**Cc:** Bill Byars; John Carmichael; Martha Roof; Robert Ward
**Subject:** SCDC Information Security

Mr. Pitts,

Mr. Carmichael asked me to send you some information regarding our information security review and the steps we have taken to secure personal and confidential information. Attached is a summary of the types of personal information we maintain and the related policies and security practices we have in place. Also attached is our main policy related to the security, acceptable use, and confidentiality of electronic data. This policy has been updated recently and is in the process of being reviewed. The last attachment is the questionnaire used in the evaluation by the Office of the Inspector General, including our responses.

Please let me know if you have any questions or need more information.

*Trevis Shealy*
*Division Director, Resource and Information Management*
*South Carolina Department of Corrections*
*803-896-2095*

## Godfrey, Rob

**From:** Patel, Swati
**Sent:** Thursday, October 25, 2012 11:36 AM
**To:** Godfrey, Rob; Soura, Christian; Pitts, Ted
**Cc:** Soura, Christian; Schimsa, Rebecca
**Subject:** 2012-xx Reviewing IT Security
**Attachments:** 2012-xx Reviewing IT Security.docx

This is the final draft.

Becca will put in final form if and when we get the green light.

**Godfrey, Rob**

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

Rob,

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

Thanks,
Derham

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

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

*Hacker illegally obtained credit card and Social Security numbers*

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

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

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

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

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

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

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

--

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

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

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

For Immediate Release:

October 26, 2012

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

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

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

*Hacker illegally obtained credit card and Social Security numbers*

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

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

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

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

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

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

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

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

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

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

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

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

###

# Chronology

**October 10:**

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

**October 11:**

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

**October 12:**

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

**October 15:**

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

**October 16:**

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

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

**October 18:**

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

**October 19:**

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

**October 20:**

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

**October 21-25:**

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

**Safety Precautions:**

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

# Consumer Safety Solutions

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

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

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

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

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

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

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

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

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

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

**Credit Bureaus**

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

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

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

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

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

**Credit Bureaus**

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

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

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

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

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

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

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

# Cabinet Agency Information Security Policy Highlights

## Department of Commerce

The South Carolina Department of Commerce has:

- Updated its confidentiality agreement with all employees to include social media
- Requires employees will sign a new agreement every year as part of their EPMS process
- Has consulted with the Inspector General's Office to review policies and procedures

## Department of Corrections

General IT security measures have been implemented to protect all of the agency's data resources. These are detailed in the sections below, based on the guidelines found in the Information Security Policy developed by the South Carolina Information Technology Solutions Committee.

Access Control and Personnel Security:

- Acceptable Use Policy – SCDC Policy ADM-15.05 Security of and Access to Information Technology details the acceptable use of all SCDC information technology systems, with specific sections regarding use of the internet and internet e-mail. Users must consent to the acceptable use policy each time they sign on to the internet filter.
- User Authentication – Each SCDC staff member has a single user id and password to access all SCDC systems and applications. Since users do not have to remember different user IDs and passwords, they are not tempted to write them down or use passwords that are easy to
- Security Awareness Program – Security training is provided in new employee orientation and is reinforced with computer based training and regular communications through agency wide e-mail, intranet news postings, and employee newsletter articles.
- Role Based Security – SCDC policy requires that access to data and applications be requested by a Warden, Division Director, or higher authority and approved by the appropriate "data owner". For example, access to medical records may only be granted upon the approval of the Division of Health Services.
- Account Deactivation – Procedures are in place to remove user accounts when employees leave the agency and review all application and data access when employees move from one position to another within the agency.

Network Security:

Firewall configured using security industry best practices by specialists at the Division of State Information Technology (DSIT). Firewall service module provides hardware redundancy.

All inbound traffic denied unless specifically allowed:

- Internet web site and web applications
- IP videoconferencing gatekeeper
- Inbound e-mail
- Remote access via Virtual Private Network (VPN)

Remote Access

- Provided primarily via web services such as SSL encrypted web
- applications, Outlook Web Access, ActiveSync, etc.
- Remote network access restricted to only those employees required to
- support network devices.
- SSL encrypted VPN tunnels allowed only to specific network
- segments required for network support.

Internet Content Filter

- Requires authentication and consent to acceptable use policy for
- internet access.
- Blocks inappropriate content and logs all internet browsing sessions.
- Scans all incoming files for viruses and other forms of malware.
- Provides a browser based malware removal tool.

E-Mail Gateway and SPAM filter

- Filters e-mail using real-time blacklists and drops messages from mail
- servers known to propagate unsolicited bulk e-mail (SPAM).
- Assigns each remaining message a score based on the probability it is
- SPAM and tags or drops messages that exceed defined thresholds.
- Scans all email attachments for viruses and other forms of malicious
- software.
- Confidential data may be sent to those outside the SCDC network via
- encrypted email by specifying [ENCRYPT] anywhere in the subject
- line
- Data Leak Prevention monitors outgoing email messages to detect
- certain data patterns, such as social security numbers (xxx-xx-xxxx).

Network Segregation

- User access layer is segregated from server, storage,and other IT infrastructure network segments.

Network Monitoring

- Automated network monitoring is in place for all servers, routers, and
- other critical IT infrastructure.
- SCDC staff actively monitors network bandwidth for signs of
- suspicious activity.
- Intrusion Detection System (IDS) sensor installed inside SCDC
- Network provides daily reports to SCDC and SC-ISAC (DSIT centr

## Department of Employment and Workforce

DEW performs the following functions as part of normal business process to prevent Personally Identifiable Information data loss:

- 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
- 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.
- Sensitive areas with PII are accessed by key card only

Actions taken after the DHHS breach:

- All remote access by employees is secured using 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.

## Department of Health and Human Services

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.

## Department of Juvenile Justice

The 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. 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.

- 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.

## Department of Labor, Licensing and Regulation

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.

The following were 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.

## Department of Motor Vehicles

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

- 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.
- With respect to our relational database, we have three specific safeguards upon which we rely heavily:
    - A person accessing our database must have 'authorization' to enter into the database.
    - A person entering the database must be connecting from a known IP address.
    - All database transactions are monitored and filed thus establishing a 'fingerprint system' by name of all who were inside the database.
- All SCDMV employees undergo an internal state background investigation prior to offer of employment.
- We have implemented a 'strong password' system across the agency which mitigates casual use by a fellow employee.
- 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.
- 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.

## Department of Parks, Recreation and Tourism

Special actions taken since April 2012 include:

- Removed employee SSN from all HR / personnel paperwork (EPMS, leave forms, etc).
- When selected vendors for point-of-sale and reservation system required that they be PCI compliant.
- PRT does not capture or store any credit card numbers – all information is encrypted and sent to vendors.

## Department of Probation, Parole and Pardon Services

Protection measures include:

- Department personnel may only access the data system upon granting of security level rights, restricted 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
- 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.

Pending strategies to enhance data security include:

- 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.

## Department of Public Safety

SCDPS' status as a law enforcement agency requires the establishment of clear and explicit standards on appropriate and acceptable uses of computer resources and information systems:

- 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.
- 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.

The 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.

## Department of Transportation

- Stopped using Social Security numbers when acquiring data for certain agency functions, for example: requesting a parking space.
- 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.
- Implemented strong password policy that requires renewal every 90 days.

## Department of Juvenile Justice

The 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. 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.

- 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.

## Godfrey, Rob

**From:** Smith, Glenn <gsmith@postandcourier.com>
**Sent:** Monday, October 29, 2012 2:30 PM
**To:** Godfrey, Rob
**Subject:** FOIA request
**Attachments:** Hacking FOIA Governor.docx

Rob,
Attached is a FOIA request related to the hacking of DOR computers. Thanks in advance for your assistance with this matter.

Glenn Smith
Reporter
The Post and Courier
134 Columbus Street
Charleston, SC 29403
843-937-5556
843-937-5579 (fax)
www.postandcourier.com/staff/glenn_smith/

## Godfrey, Rob

**From:** Phillips, Noelle <nophillips@thestate.com>
**Sent:** Tuesday, October 30, 2012 1:08 PM
**To:** Godfrey, Rob
**Subject:** Re: FW: FOI request

Thanks.

On Tue, Oct 30, 2012 at 12:58 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

Noelle,

I have forwarded your email to the appropriate person in our office.

Rob

**From:** Phillips, Noelle [mailto:nophillips@thestate.com]
**Sent:** Tuesday, October 30, 2012 12:58 PM
**To:** Samantha Cheek
**Cc:** Godfrey, Rob
**Subject:** FOI request

Samantha,

I've attached an FOI letter to this email. If you have any questions, call or send an email. Thanks.

--
Noelle Phillips

Reporter

The State Media Co.

(803) 771-8307

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

## Godfrey, Rob

**From:** LeMoine, Leigh
**Sent:** Thursday, October 25, 2012 7:54 PM
**To:** Godfrey, Rob; Pitts, Ted
**Subject:** RE: Talking points

Ted- are you going to send these over to NH to review?

Leigh

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

**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.

## Godfrey, Rob

**From:** Emily Brady <Emily.Brady@chernoffnewman.com>
**Sent:** Wednesday, October 24, 2012 10:00 PM
**To:** Godfrey, Rob
**Cc:** Rick Silver; Tim Kelly
**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:** Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Sent:** Wednesday, October 24, 2012 6:32 PM
**To:** Godfrey, Rob; Emily Brady
**Cc:** Rick Silver
**Subject:** RE: Experian question

Just email it to us.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Wednesday, October 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:** Emily Brady <Emily.Brady@chernoffnewman.com>
**Sent:** Wednesday, October 24, 2012 6:27 PM
**To:** Godfrey, Rob
**Cc:** Rick Silver; Tim Kelly
**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:** Emily Brady <Emily.Brady@chernoffnewman.com>
**Sent:** Wednesday, October 24, 2012 10:29 PM
**To:** Godfrey, Rob
**Cc:** Rick.Silver@chernoffnewman.com; Tim.Kelly@chernoffnewman.com
**Subject:** Re: Experian question

Great- thanks!

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

On Oct 24, 2012, at 10:27 PM, "Godfrey, Rob" <RobGodfrey@gov.sc.gov> wrote:

> 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:** Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Sent:** Thursday, October 25, 2012 11:38 AM
**To:** Godfrey, Rob
**Attachments:** SC Department of Revenue Investigating Data Breach.docx

Rob, this is still a draft that's very much in flux, but wanted you to have it before we walk over.

**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

# 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 387,000 credit card and 3.3 million Social Security numbers have been compromised in a cyber attack. As a result, state officials will provide any affected taxpayer with one year of credit monitoring and identity theft protection. Officials emphasized that no public funds were accessed or put at risk.

Of the credit cards, 371,000 are protected by strong encryption deemed sufficient under the demanding credit card industry standards to protect the data and cardholders, and the others dated from before 2003.

"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 15, 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 www.1111111.com or call 1-800-XXX-XXXX beginning XXXXXX to determine if their information is affected. If so, the taxpayer can immediately enroll in one year of Experian's ProtectMyID™ Alert , an identity protection service, to detect, protect and resolve potential identity theft.

In addition to the Experian service, state officials urged individuals to take 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.

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

Governor Haley has tasked the Inspector General with....

## Godfrey, Rob

**From:** Emily Brady <Emily.Brady@chernoffnewman.com>
**Sent:** Thursday, October 25, 2012 2:14 PM
**To:** Godfrey, Rob
**Cc:** Tim.Kelly@chernoffnewman.com; Rick.Silver@chernoffnewman.com
**Subject:** Re: What do y'all need from me this afternoon?

Feedback on documents we shared with you earlier.

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

On Oct 25, 2012, at 2:12 PM, "Godfrey, Rob" <RobGodfrey@gov.sc.gov> wrote:

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

## Godfrey, Rob

**From:** Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Sent:** Thursday, October 25, 2012 3:42 PM
**To:** Godfrey, Rob; Rick Silver; Emily Brady
**Subject:** RE: What do y'all need from me this afternoon?

Rob, can I get some of the language in that executive order yet for inclusion in the release?

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Thursday, October 25, 2012 2:15 PM
**To:** Tim Kelly; Rick Silver; Emily Brady
**Subject:** RE: What do y'all need from me this afternoon?

Thanks y'all.

**From:** Tim Kelly [mailto:Tim.Kelly@chernoffnewman.com]
**Sent:** Thursday, October 25, 2012 2:14 PM
**To:** Godfrey, Rob; Rick Silver; Emily Brady
**Subject:** RE: What do y'all need from me this afternoon?

We're working on tightening up Jim's statement with the lawyers, and then we'll make it consistent with press release and timeline. We'll get you some stuff to look at in a bit.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Thursday, October 25, 2012 2:11 PM
**To:** Tim Kelly; Rick Silver; Emily Brady
**Subject:** What do y'all need from me this afternoon?

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

## Godfrey, Rob

**From:** Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Sent:** Thursday, October 25, 2012 6:22 PM
**To:** Godfrey, Rob
**Subject:** Emailing: DOR.pdf
**Attachments:** 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:

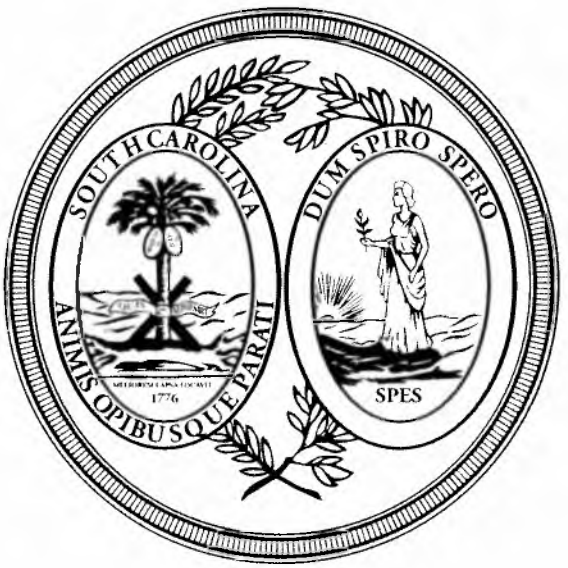
DOR.pdf

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.

# For More Information:

## Call Toll Free 1-866-578-5422

## Visit protectmyid.com/scdor



## Godfrey, Rob

**From:** Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Sent:** Thursday, October 25, 2012 9:41 PM
**To:** Rick Silver; Godfrey, Rob; Emily Brady; etter_jf@sctax.org; Samantha Cheek; Harry Cooper; Rush Smith; jon.neiditz@nelsonmullins.com; marshall.heilman@mandiant.com
**Subject:** Press Kit
**Attachments:** DORMeda.zip

<<DORMeda.zip>> The draft media kit materials are attached. We'll add DOR letterhead to the release in the morning. Rob will need a draft for Chief Keel by 8:30, and I'll need final approval of everything by 9 to get everything assembled for the press conference.

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



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

DORMeda.zip

## Godfrey, Rob

**From:** Tim Kelly <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@nelsonmullins.com; ofonseca@experianinteractive.com
**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

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:** Ozzie Fonseca <ofonseca@experianinteractive.com>
**Sent:** Friday, October 26, 2012 8:10 AM
**To:** Tim Kelly; Godfrey, Rob; Rick Silver; Jim Etter; Harry Cooper; Samantha Cheek; Liz Mason
**Cc:** Rush Smith; jon.neiditz@nelsonmullins.com
**Subject:** RE:
**Attachments:** image001.jpg; image002.png; image003.png; image004.png

The information, as it relates to ProtectMyID Alert, has been approved.

One suggestion is to remove the word "any" from the phrase "any suspicious activity" (the term may be too broad).

Thanks

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

Experian Consumer Services
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/DBBlog<http://www.experian.com/DBBlog>
Follow us on Twitter: www.Twitter.com/Experian_DBR<http://www.twitter.com/Experian_DBR>
Visit us at http://www.experian.com/databreach



---

From: Tim Kelly [Tim.Kelly@chernoffnewman.com]
Sent: Friday, October 26, 2012 4:49 AM
To: Godfrey, Rob; Rick Silver; Jim Etter; Harry Cooper; Samantha Cheek; Liz Mason
Cc: Rush Smith; jon.neiditz@nelsonmullins.com; Ozzie Fonseca
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

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

1411 Gervais Street
Columbia, SC 29201

## Godfrey, Rob

**From:** Tim Kelly <Tim.Kelly@chernoffnewman.com>
**Sent:** Friday, October 26, 2012 9:18 AM
**To:** Godfrey, Rob; Rick Silver; Emily Brady
**Subject:** RE: Executive Order 2012-10 and Letter to Maley

Thanks

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Friday, October 26, 2012 9:15 AM
**To:** Tim Kelly; Rick Silver; Emily Brady
**Subject:** Executive Order 2012-10 and Letter to Maley

## Godfrey, Rob

**From:** Emily Brady <Emily.Brady@chernoffnewman.com>
**Sent:** Friday, October 26, 2012 9:29 AM
**To:** Godfrey, Rob
**Subject:** RE: Press Conference

Great- thanks

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**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

## Godfrey, Rob

**From:** LeBlanc, Clif <cleblanc@thestate.com>
**Sent:** Sunday, October 28, 2012 6:25 PM
**To:** Godfrey, Rob; Clif LeBlanc
**Subject:** Re: What's up? Unable to get to a phone right now

Rob,

Mr. Etter has told WIS that it will take "a few days" before a taxpayer who has submitted his/her name to the protectmyid.com web site to learn whether their tax records were misused and therefore subject to the one year free credit monitoring. Is that the case, and, if so, how long is a few days (2, 3, 5, 10)?

Has state govt. decided to do anything beyond what was announced Friday, such as adding for phone lines, more people to answer calls, or any similar means of providing quicker responses to taxpayers?

When will the state/Mandiant know where the hacker(s) got access to full tax returns that include addresses, children's names, charitable giving, tax delinquencies, etc.?

Clif

On Sun, Oct 28, 2012 at 6:03 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

Clif,

As far as I know Director Etter isn't doing a media round today - he's currently working on making sure that everything that needs to happen to protect taxpayers is being done. He's going to be at the press conference tomorrow precisely to answer and question's y'all have. But, if there's anything you think you need to know tonight, I'll get it answered for you.

If you have any questions or concerns related to the call center that has been set up to assist taxpayers, I will make sure you are set up to talk to Experian as soon as possible.

As to the timing, there is information we believe is important to get out to the taxpayers, and 10:00 AM is the best time to make sure the press has the time y'all need to put it out by the noon news. We are, as we have been, in constant contact with the legislative leadership, we'll remain in constant contact with members, and we'll brief them at the first available opportunity tomorrow morning. It won't be long after 10, and it may be before if it works for them.

In the meantime, every South Carolinian should call the number (information below) and avail themselves of the free protections the state is offering, and they should do it sooner rather than later. Remember, as the governor said Friday, although we have been attacked, we aren't going to be victims.

Again, thanks for reaching out.

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 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.

---

**From**: LeBlanc, Clif [mailto:cleblanc@thestate.com]
**Sent**: Sunday, October 28, 2012 05:50 PM
**To**: Godfrey, Rob
**Subject**: Re: What's up? Unable to get to a phone right now

Your DOR director is doing media interviews, I'd like to talk to him this afternoon.

In addition, what are y'all doing about the conflicting times for Monday's news conference and the phone conference for legislators?

Clif LeBlanc

On Sun, Oct 28, 2012 at 5:46 PM, Godfrey, Rob <RobGodfrey@gov.sc.gov> wrote:

## Godfrey, Rob

**From:** Greg Young <Greg.Young@experianinteractive.com>
**Sent:** Monday, October 29, 2012 1:04 PM
**To:** Godfrey, Rob
**Subject:** RE: Referred by Rob Godfrey

Reviewing release now....on con call. Will call as soon as this hangs up.

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: Monday, October 29, 2012 10:02 AM
To: Greg Young
Subject: RE: Referred by Rob Godfrey
Importance: High

Greg -

Call me.

Rob

## Godfrey, Rob

**From:** Thad Westbrook <thad.westbrook@nelsonmullins.com>
**Sent:** Monday, October 29, 2012 1:10 PM
**To:** Godfrey, Rob
**Subject:** RE: For review

We've reviewed it. Call me when you can.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 12:52 PM
**To:** Thad Westbrook
**Subject:** For review

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

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

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

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

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

- For anyone who wishes to bypass the telephone option, there is an online service available at http://www.protectmyid.com/scdor. Enter the code **SCDOR123** when prompted. Every South Carolina taxpayer who takes the time to sign up will be afforded the protection, and that protection is retroactive. South Carolina taxpayers have until the end of January, 2013 to sign up. South Carolina taxpayers who sign up for protection will be notified about how to sign up for a "Family Secure Plan" if they claim minors as dependents.

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

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

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

- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated,

U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.

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

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

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

## Godfrey, Rob

**From:** Emily Brady <Emily.Brady@chernoffnewman.com>
**Sent:** Monday, October 29, 2012 3:12 PM
**To:** Godfrey, Rob
**Subject:** RE: Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter to hold press conference TUESDAY

Rob- is there another strategy meeting/call set up to discuss this among communications crowd?

Thanks,
Emily

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 2:44 PM
**Subject:** Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter to hold press conference TUESDAY

# Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter to hold press conference TUESDAY

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

**COLUMBIA, S.C.** – Governor Nikki Haley, South Carolina Law Enforcement Division (SLED) Chief Mark Keel and South Carolina Department of Revenue (DOR) Director Jim Etter will hold a press conference on Tuesday, October 30, at 9:15 AM to update the people of South Carolina on the DOR information security breach and discuss what every South Carolinian can and should do to protect themselves.

The press conference will be held in the first floor lobby of the Statehouse.

**WHO:** Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter

**WHAT:** DOR information security breach update

**WHEN:** TUESDAY, October 30, 9:15 AM

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

-###-

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

## Godfrey, Rob

**From:** Randy Grant <RGRANT@scdjj.net>
**Sent:** Wednesday, October 24, 2012 1:47 PM
**To:** Godfrey, Rob; Pitts, Ted
**Cc:** Margaret Barber
**Subject:** Information Security

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.

Should you have questions or need additional information regarding this, please address they by reply e-mail or by phone at the points of contact information below, or to my personal cell phone (803) 269-6864.

Randy

G. Randall Grant
State House Liaison
SC Department of Juvenile Justice
Goldsmith Building, Room 114
Columbia, SC 29212
rgrant@scdjj.net
(803) 896-9743

## Godfrey, Rob

**From:** Holly Pisarik <Holly.Pisarik@llr.sc.gov>
**Sent:** Wednesday, October 24, 2012 2:04 PM
**To:** Pitts, Ted; Godfrey, Rob
**Subject:** LLR Security Measures

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.

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 2:24 PM
**To:** Godfrey, Rob
**Subject:** DOT Info

**Importance:** High

**From:** Nicholas, Wendy [mailto:NicholasWB@dot.state.sc.us]
**Sent:** Wednesday, October 24, 2012 2:16 PM
**To:** Pitts, Ted
**Subject:** Info Requested
**Importance:** High

- 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.

Wendy Nicholas, Chief of Staff
South Carolina Department of Transportation
(803) 737-0885 [office]
(803) 727-6501 [cell]

**Godfrey, Rob**

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 2:24 PM
**To:** Godfrey, Rob
**Subject:** FW: SCDMV IT protections

**From:** Shwedo, Kevin A [mailto:Kevin.Shwedo@scdmv.net]
**Sent:** Wednesday, October 24, 2012 2:20 PM
**To:** Pitts, Ted
**Subject:** SCDMV IT protections

Ted - 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.

**Kevin A. Shwedo**
**Executive Director**
**South Carolina Department of Motor Vehicles**
**10311 Wilson Boulevard**

**Post Office Box 1498**
**Blythewood, South Carolina 29016**

**(O) 803-896-8925**
**(C) 803-609-4218**

**Your SCDMV -- Each a Role Model; Competent, Committed, Courteous!**

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:10 PM
**To:** Godfrey, Rob
**Subject:** Fw: Info requested - PRT

**From**: Amy Duffy [mailto:aduffy@scprt.com]
**Sent**: Wednesday, October 24, 2012 03:20 PM
**To**: Pitts, Ted
**Subject**: Info requested - PRT

Hi Ted –

Our two examples are:

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.)

PRT doesn't really deal with any sensitive, or personal, information from our customers or employees ~~ that is why we can only come up with 2 examples.

Thanks!

**Amy D. Duffy**
Chief of Staff
SC Department of Parks, Recreation & Tourism
1205 Pendleton Street, Suite 248
Columbia, South Carolina 29201

phone: (803) 734-3272
fax: (803) 734-1409
email: aduffy@scprt.com
www.discoversouthcarolina.com

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:11 PM
**To:** Godfrey, Rob
**Subject:** Fw: PII Information

----- Original Message -----
From: Lowder, Joe [mailto:JLowder@dew.sc.gov]
Sent: Wednesday, October 24, 2012 03:15 PM
To: Pitts, Ted; Turner, Abraham <ATurner@dew.sc.gov>
Subject: PII Information

Ted,

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

## Godfrey, Rob

**From:** Pitts, Ted
**Sent:** Wednesday, October 24, 2012 4:12 PM
**To:** Godfrey, Rob
**Subject:** Fw: Security changes

**From**: Huffman, Chris [mailto:chuffman@sccommerce.com]
**Sent**: Wednesday, October 24, 2012 02:47 PM
**To**: Pitts, Ted
**Cc**: Hitt, Bobby <bhitt@commerce.state.sc.us>; Patrick, George <gpatrick@sccommerce.com>
**Subject**: Security changes

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

## Godfrey, Rob

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

Done.

Samantha Cheek

SC Department of Revenue

(803) 898-5281

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

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

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:** Shane Massey <[redacted]@bellsouth.net>
**Sent:** Friday, October 26, 2012 4:45 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

Ah, I thought it was call the center **OR** go online. It's actually both. Thanks, Rob.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**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:[redacted]@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:** Jim Etter <Etter_JF@sctax.org>
**Sent:** Saturday, October 27, 2012 3:32 PM
**To:** Godfrey, Rob
**Subject:** Post and courier

Had a good conversation with Diette

Sent from my iPhone

## Godfrey, Rob

**From:** Samantha Cheek <CheekS@sctax.org>
**Sent:** Sunday, October 28, 2012 1:01 PM
**To:** Godfrey, Rob
**Cc:** [redacted]@gmail.com
**Subject:** Re: Phone interview

I've already spoken with him at 11 this morning. Basic questions about the situation and protection program...

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

On Oct 28, 2012, at 12:23 PM, "Godfrey, Rob" <RobGodfrey@gov.sc.gov> wrote:

> Samantha,
>
> Please reach out to the reporter and figure out what questions they have. Submit answers to them in writing. Shoot the written answers my way, and we'll sign off.
>
> Rob
>
> ----- Original Message -----
> From: Jim Etter [mailto[redacted]@gmail.com]
> Sent: Sunday, October 28, 2012 12:14 PM
> To: Samantha Cheek <CheekS@sctax.org>
> Cc: Godfrey, Rob
> Subject: Re: Phone interview
>
> Ron,
> Are handling this????
> Jim
>
> Sent from my iPhone
>
> On Oct 28, 2012, at 10:27 AM, "Samantha Cheek" <CheekS@sctax.org> wrote:
>
>> Later this morning with WPDE to answer questions.
>>
>> Samantha Cheek
>> SC Department of Revenue
>> (803) 898-5281

## Godfrey, Rob

**From:** Haltiwanger, Katherine
**Sent:** Monday, October 29, 2012 9:31 AM
**To:** Godfrey, Rob
**Cc:** Pitts, Ted
**Subject:** Voicemail

Rob,

Here is one voicemail I wanted to pass along that was on your machine…

Catherine Salazar, Info. Security Director at the DOR in the State of AZ, 602.316.5714. She requested a confidential briefing.

-Katherine

## Godfrey, Rob

**From:** Jim Etter <Etter_JF@sctax.org>
**Sent:** Monday, October 29, 2012 1:11 PM
**To:** Godfrey, Rob
**Cc:** Harry Cooper
**Subject:** Fwd: SC Department of Revenue Cyber Attack

Do you us to respond

Sent from my iPhone

Begin forwarded message:

> **From:** "Harry Cooper" <COOPERH@sctax.org>
> **Date:** October 29, 2012, 12:56:14 PM EDT
> **To:** "Jim Etter" <Etter_JF@sctax.org>
> **Subject: FW: SC Department of Revenue Cyber Attack**
>
> ...do you want to reply?
>
> ---
>
> **From:** Tom Britt [mailto:tomb@bankoftravelersrest.com]
> **Sent:** Monday, October 29, 2012 12:16 PM
> **To:** Director
> **Cc:** Harry Cooper; Alvin "Mont" Alexander; watts@sctax.org; Nancy Wilson; Sherrie McTeer; Meredith Cleland; Mike Garon; kimpsom@sctax.otg; Rick Handel; Kimberly Haley
> **Subject:** SC Department of Revenue Cyber Attack
>
> Director Etter:
>
> I work for Bank of Travelers Rest in Travelers Rest, SC. I have a question I need to help our customers with, the questions is: Where the bank account numbers and bank routing numbers of our Customers, your Taxpayers compromised in this Cyber Attack? As you know when Taxpayers get a refund from the State many times they have the money deposited directly into their checking account-this is done with the information, bank account number and bank routing number provided by the Taxpayer to the State this potentially seems to be the most dangerous concern other than Social Security Numbers being breached. With SS#'s and bank account numbers and routing numbers a lot of damage can be done. How do we respond to our customers? Many of our customers depend on the Bank of Travelers Rest for all of their financial advice and many of our customers are very scared and concerned, we want to direct them in a professional and accurate manor.
>
> An immediate response would be greatly appreciated. The 1-866-578-5422 phone number I cannot get through, the last time I tried it simply hung up or the line went dead.
>
> Thanks for your time and look forward to hearing from you!
>
> Tom Britt
> Executive Vice President
> 864-660-7638

## Godfrey, Rob

**From:** McManus, Ken
**Sent:** Monday, October 29, 2012 3:14 PM
**To:** Godfrey, Rob
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

Rob: Once again, thanks for these. I forwarded the one from last week on this topic to another OEPP Director and his response was, "Wow. Great information. Shouldn't all the directors be getting these?" Thanks to you, I get to hear from the Governor via video on all these matters of great importance, but most of my colleagues do not. Also, many of our friends and neighbors think we in OEPP work more closely with the Governor than we do. When asked about issues, I find it useful to be able to forward these messages to them, so that they can hear the Governor in her own words. They will watch something I send them, but otherwise rely on media sound bites. Your thoughts? Ken McManus

**From:** Godfrey, Rob
**Sent:** Monday, October 29, 2012 1:22 PM
**Subject:** Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

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

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

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

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

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

- For any South Carolina taxpayer residing in South Carolina who wishes to bypass the telephone option, there currently is an online service available at http://www.protectmyid.com/scdor. Enter the code **SCDOR123** when prompted. Every South Carolina taxpayer who takes the time to sign up will be afforded the protection, and that protection is retroactive. South Carolina taxpayers have until the end of January, 2013 to sign up. South Carolina taxpayers who sign up for protection will be notified about how to sign up for a "Family Secure Plan" if they claim minors as dependents.

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

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

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

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

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

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

-###-

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

## Godfrey, Rob

**From:** Samantha Cheek <CheekS@sctax.org>
**Sent:** Monday, October 29, 2012 3:48 PM
**To:** Godfrey, Rob
**Subject:** RE: Have y'all removed my numbers from website?

....Still trying to get someone from IRM to do this ASAP.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 3:46 PM
**To:** Samantha Cheek
**Subject:** Have y'all removed my numbers from website?

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

## Godfrey, Rob

**From:** Samantha Cheek <CheekS@sctax.org>
**Sent:** Monday, October 29, 2012 4:02 PM
**To:** Godfrey, Rob
**Subject:** FW: WIS request

Carrie will be handling this one solo.

**From:** Till, Shana [mailto:shanatill@wistv.com]
**Sent:** Monday, October 29, 2012 3:14 PM
**To:** Samantha Cheek
**Subject:** WIS request

Hi Samantha!

We are dedicating an hour of newstime tomorrow to answer viewer questions about the hack.
Carri with Consumer Affairs will be in our studios to answer questions on air – and we'll also have an online chat going.
Would be available for interview tomorrow as well? We're starting at 5:00 p.m.
We'd love to have you. Thanks so much!

**Shana Till**
Assistant News Director
O: (803) 758-1165
C: (803) 608-5726
shanatill@wistv.com
Follow Us On Twitter - @WIS10

## Godfrey, Rob

**From:** Samantha Cheek <CheekS@sctax.org>
**Sent:** Monday, October 29, 2012 3:52 PM
**To:** Godfrey, Rob
**Subject:** Tim Smith

Followed up.

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

## Godfrey, Rob

**From:** Fairwell, Adrienne <AFairwell@dew.sc.gov>
**Sent:** Wednesday, October 31, 2012 9:37 AM
**To:** Godfrey, Rob
**Subject:** RE: Executive order

Got it; thx!

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Wednesday, October 31, 2012 9:34 AM
**To:** Fairwell, Adrienne
**Subject:** Executive order

http://governor.sc.gov/ExecutiveOffice/Documents/2012-10%20Reviewing%20IT%20Security.pdf

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

## Godfrey, Rob

**From:** Adcox, Seanna M. <SAdcox@ap.org>
**Sent:** Wednesday, October 31, 2012 12:43 PM
**To:** Godfrey, Rob
**Subject:** Email request

Can I get copies of Gov. Haley's emails since Sept. 13 that reference or in any way pertain to the security breach at the Department of Revenue. Also, on the same subject and time frame, copies of emails written or received by Tim Pearson and Bryan Stirling.

Seanna



msk dccc60c6d2c3a6438f0cf467d9a4938

## Godfrey, Rob

**From:** Jacoby, Marybeth <mjacoby@WLTX.GANNETT.COM>
**Sent:** Wednesday, October 31, 2012 1:38 PM
**To:** Godfrey, Rob
**Subject:** RE: Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter to hold press conference TODAY

Rob,
Thanks we will be there but is there a little more you can tell me about content?

*Marybeth*

**Marybeth Jacoby**

**News Director**

News 19, WLTX and online

6027 Garners Ferry Road

Columbia, SC 29209

Work: 803.647.0231

Mobile: 803.429.5268

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Wednesday, October 31, 2012 1:24 PM
**Subject:** Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter to hold press conference TODAY

# Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter to hold press conference TODAY

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

**COLUMBIA, S.C.** – Governor Nikki Haley, South Carolina Law Enforcement Division (SLED) Chief Mark Keel and South Carolina Department of Revenue (DOR) Director Jim Etter will hold a press conference **TODAY, Wednesday, October 31, at 4:30 PM** to update the people of South Carolina on the DOR information security breach. The press conference will be held in the first floor lobby of the Statehouse.

**WHO:** Gov. Nikki Haley, SLED Chief Mark Keel, DOR Director Jim Etter

**WHAT:** DOR information security breach update

**WHEN:** TODAY, Wednesday, October 31, 4:30 PM

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

-###-

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

## Godfrey, Rob

**From:** Rep. Bill Taylor <bill@taylorschouse.com>
**Sent:** Wednesday, October 31, 2012 3:53 PM
**To:** Godfrey, Rob
**Subject:** SC 's HACKED - FAQs



# HACKING - FAQs

(Informational Newsletter)

Dear Friends:

I trust you're keeping up-to-date on the S.C. cyber hacking situation through various news media reports. As you know, the Department of Revenue's computer system was hacked and 3.6 million Social Security numbers were stolen along with nearly 400,000 credit card numbers. This is a troubling situation for every South Carolinian and for state government. Every day there are new developments with more questions. To help provide answers, here are the most Frequently Asked Questions:

**How bad is the situation?**
Information hacked from DOR could haunt SC taxpayers for years to come. Hackers could have in their possession taxpayer information that would allow crooks to take over bank accounts, file for bogus tax refunds or get fraudulent loans. One security analyst was quoted. "This is about the worst you can get."

**How do I sign up for credit monitoring?**
Anyone who has filed a South Carolina tax return since 1998 should visit http://www.protectmyid.com/scdor and enter the code **"scdor123"** to enroll in one year of credit monitoring provided by Experian. **You need to click the button** that says **"Click to redeem your activation code"** instead of pressing enter. Or, call 1-866-578-5422 to determine if your information is affected and to enroll in one year of credit monitoring provided by Experian.

**Could we not have a portal provided that would allow quicker, more direct and easier access?**
Based on my experience today, using the Experian website is easy; it took me about two minutes to complete the form. A way to confirm that you are on the correct page is the picture of the person/model on the page should be a female. Some people are being bounced directly to the Experian home page (the picture on this page is a male) this is a problem on the user's end not Experian's. If you don't have access to the internet, please call 1-866-578-5422. The wait times are getting shorter.

**Why was it so difficult to get through on the phone lines over the weekend?**
Even with 300+ phone operators, the Experian call center was overwhelmed. To alleviate the

congestion the code "**scdor123"** was made available publically rather than forcing people to call the phone center.

**What's my protection against future fraud?**
Experian's ProtectMyID™ Alert is designed to detect, protect, and resolve potential identity theft and includes daily monitoring of all three credit bureaus.

**How long will state government protect me from fraud?**
Under a deal negotiated with a credit monitoring agency Experian, SC citizens whose tax returns were hacked will be eligible for credit fraud resolution for life.

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

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

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

**Were checking account routing numbers compromised?**
Of the files accessed an individual's entire return was accessed. The Social Security #'s and bank information were not encrypted. Credit cards were encrypted on returns after 2003. Any unencrypted credit card information would be for cards that have expired.

**Were business accounts compromised?**
The state DOR doesn't know if business accounts were compromised by a hacker who broke into the agency's computer files of tax returns. As the investigation is still ongoing, a DOR spokesperson says it cannot determine at this time exactly who was affected.

**What about my credit card I had on file with DOR?**
DOR says that the vast majority of credit cards are protected by strong encryption, but about 16,000 of the card numbers are not encrypted.

**Why wasn't the DOR database information encrypted?**
The state had used the same standards as banks and other private institutions when it decided not to encrypt your data. The state has now opted to begin encrypting all of the agency's files - a process that should be completed in the next several months. Increasing security for all of the state's informational technology has also become a priority.

**Should we be concerned with scammers taking advantage of the situation?**
Yes! One constituent wrote me that she received two e-mails already from what appeared to be American Express asking for her to update some of her information. She says the Web Site looked OK, but the information requested was too detailed. She didn't fall for the scam and instead called Amex. They confirmed both emails are from hackers. Amex has put a fraud alert on her account. We all have to be personally vigilant and smart.

**Who is to blame?**
Sophisticated international cyber crooks are at fault. No one at DOR has been cited for being at fault. A senate legislative committee is investigating.

**What's being done to see this doesn't happen again?**

Gov. Haley has signed an executive order directing all of her Cabinet agencies to designate someone to cooperate with state Inspector General Patrick Maley on a new effort to improve the state's cyber-security. She's stated, "State government's fragmented approach to IT security makes South Carolina vulnerable to serious cyber and information breaches,"

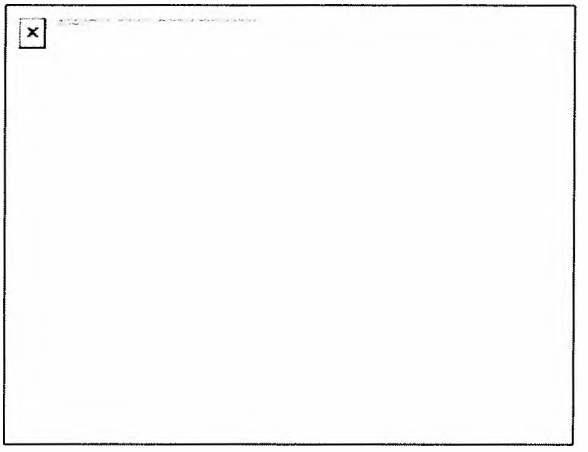
***More Questions?***
These FAQ's don't answer everything, so if you have a question send it to me and I'll do my best to get you an answer. Please be patient because with the process - it's a dynamic situation.

**OF SPECIAL NOTE:** I urge you take advantage of the protection offer by going to http://www.protectmyid.com/scdor and enter the code **"scdor123"** to enroll in one year of credit monitoring provided by Experian. You need to click the button that says "Click to redeem your activation code" instead of pressing enter. Or, call 1-866-578-5422 to determine if your information is affected and to enroll in one year of credit monitoring provided by Experian. *REMEMBER:* We all have to be personally vigilant and smart.

In your Service,
***Bill Taylor***
***803-270-2012***
Representative
South Carolina General Assembly
Bill@taylorschouse.com
www.Taylorschouse.com



**Picture of the Week**

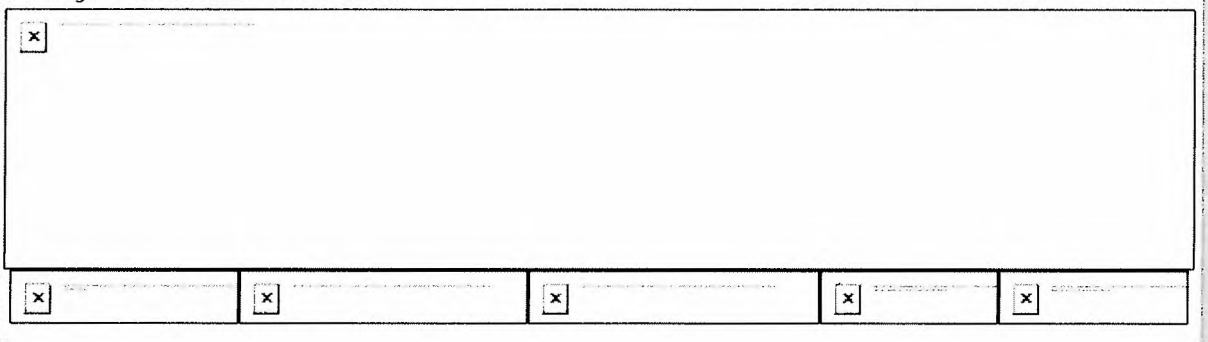


**Aiken's Vocational Rehabilitation Center is about a 'Hand Up' as opposed to a 'Hand Out'. House Candidate Don Wells and I were accompanied by Center Manager John McMurtrie on a tour of the York Street facility. These folks partner with local industries to train and re-train people who want to work. It's all about JOBS!**

## Godfrey, Rob

**From:** Rep. Bill Taylor <bill@taylorschouse.com>
**Sent:** Friday, October 26, 2012 6:26 PM
**To:** Godfrey, Rob
**Subject:** SC 's Been HACKED - This is a serious warning OPEN NOW





# SC's Been *HACKED* !

(Informational Newsletter)

Dear Friends:

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

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

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

Here's what you need to do...

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

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

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

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

**Additional steps to protect yourself...**

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

**Final Thought**

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

In your Service,

***Bill Taylor***

***803-270-2012***

Representative
South Carolina General Assembly

Bill@taylorschouse.com

www.Taylorschouse.com

Newsletter not paid for by taxpayer funds.

Paid for by TaylorSCHouse

## Godfrey, Rob

**From:** Stirling, Bryan
**Sent:** Wednesday, October 31, 2012 5:54 PM
**To:** Godfrey, Rob
**Subject:** FW: D&B Credibility Corp.

**From:** Judy Hackett [mailto:jhackett@dandb.com]
**Sent:** Wednesday, October 31, 2012 5:53 PM
**To:** Pitts, Ted
**Cc:** Aaron Stibel; Jeff Stibel; Stirling, Bryan
**Subject:** RE: D&B Credibility Corp.

Ted,

We watched the press conference. Great job by the Governor. One point of clarification is that our official name is Dun & Bradstreet Credibility Corp. The reason that's important is because we are the business that does credit monitoring for businesses. D&B focuses on other areas. We don't want your constituents confused and calling the wrong group. I have notified their press and customer support operations so that they can transfer the calls to us but it would be great if we could make that distinction clear in any future communications so that your constituents aren't transferred needlessly. We've already seen incorrect messaging come across the media wires. Perhaps we should draft a joint release of this information so that we make sure that the information is accurate and the product readily available. I have asked my PR firm to get this started just so that we have something to respond to but happy to let your team take the lead.

Judy Hackett
Chief Marketing Officer
Dun & Bradstreet Credibility Corp
22761 Pacific Coast Highway
Malibu, CA 90265
O: 310-919-2233
C: 770-337-4869
F: 310-919-2948
www.DandB.com

**Dun & Bradstreet**
CREDIBILITY CORP

**From:** Judy Hackett
**Sent:** Wednesday, October 31, 2012 12:50 PM
**To:** 'TedPitts@gov.sc.gov'
**Cc:** Aaron Stibel; Jeff Stibel
**Subject:** D&B Credibility Corp.
**Importance:** High

What we can do today:

- Dun & Bradstreet Credibility Corp will give South Carolina businesses affected, a CreditAlert product that will help them stay alerted to changes in their scores or ratings and other indicators of fraudulent activity that could be taking place on their business. The cost will be waived for residents of the state.
- They should visit DandB.com/SC starting Friday, 11-2 or they can call customer service toll free at this dedicated phone number 800-279-9881

For Background

- How does the product help? If someone were to steal your business identity, items could be purchased, your bills could go unpaid, new lines of credit could be opened up. This product will alert customers to changes taking place in their business credit file. Even something as simple as a change to a business address or a company officer change would set off an alert to the business owner.

As we mentioned on the phone, if you need anything else now or in the future, please do not hesitate to reach out.

Also If you need a quote from our CEO, feel free to use what he said on the phone:

Chairman and CEO Jeff Stibel said, "When our nation or our states are in need, Dun & Bradstreet Credibility Corp. will drop everything to help. We are honored to serve this great state and tremendous governor."

Judy Hackett
Chief Marketing Officer
Dun & Bradstreet Credibility Corp
22761 Pacific Coast Highway
Malibu, CA 90265
O: 310-919-2233
C: 770-337-4869
F: 310-919-2948
www.DandB.com

Dun & Bradstreet
CREDIBILITY CORP

**Godfrey, Rob**

**From:** Neal, Sharranda <sneal@wltx.gannett.com>
**Sent:** Wednesday, October 31, 2012 5:58 PM
**To:** Godfrey, Rob
**Subject:** Request from News19 WLTX-TV

Pursuant to the SC Freedom of Information Act, News19 WLTX-TV requests the following information:

*all email/ written correspondence between Governor Nikki Haley and her staff with Pat Malley and James Etter between August 26, 2012 to present ( October 31, 2012)
* any written requests, from Governor Nikki Haley requesting an investigation into how hackers breached the computer servers maintained by the South Carolina Department of Revenue
This request is for correspondence sent between August 26, 2012 and October 31, 2012

I request any fees associated with this request be waived, because the information requested will serve the public interest.
Please let me know if there is anything more I need to do to facilitate this request.
Thanks for your prompt response,

Sharranda Neal
Content Manager
News19 WLTX-TV
Address: 6027 Garners Ferry Road
Columbia, S.C. 29209
Phone: (803) 695-3741
Cell Phone: (803) 429-9021
Fax: (803) 776-1791

## Godfrey, Rob

**From:** Jim Etter <Etter_JF@sctax.org>
**Sent:** Saturday, October 27, 2012 2:31 PM
**To:** Godfrey, Rob
**Subject:** Contact

FYI
Sent from my iPhone

## Godfrey, Rob

**From:** Thad Westbrook <thad.westbrook@nelsonmullins.com>
**Sent:** Monday, October 29, 2012 2:24 PM
**To:** Godfrey, Rob; Stirling, Bryan
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

I'm contacting Experian about this. There should be no charge.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 1:58 PM
**To:** Stirling, Bryan; Thad Westbrook
**Subject:** FW: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

**From:** Klump, Allen [mailto:Allen.Klump@mail.house.gov]
**Sent:** Monday, October 29, 2012 1:55 PM
**To:** Godfrey, Rob
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

FYI, I just did this and it made me pay $3 for my credit report

Allen G. Klump
Communications Director
The Office of Congressman Jeff Duncan SC-3
303 West Beltline Blvd.
Anderson, SC 29625
Cell: 864-915-4059



**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 1:22 PM
**Subject:** Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

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

**COLUMBIA, S.C.** – Governor Nikki Haley, South Carolina Law Enforcement Division Chief Mark Keel and South Carolina Department of Revenue (DOR) Director Jim Etter today provided reporters with an update on the S.C. DOR information security breach and discussed consumer safety solutions available to South Carolinians during a Statehouse press conference. S.C. DOR announced on October 26, 2012 that

approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers had been exposed in a cyber attack.

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

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

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

- For any South Carolina taxpayer residing in South Carolina who wishes to bypass the telephone option, there currently is an online service available at http://www.protectmyid.com/scdor. Enter the code **SCDOR123** when prompted. Every South Carolina taxpayer who takes the time to sign up will be afforded the protection, and that protection is retroactive. South Carolina taxpayers have until the end of January, 2013 to sign up. South Carolina taxpayers who sign up for protection will be notified about how to sign up for a "Family Secure Plan" if they claim minors as dependents.

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

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

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

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

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

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

-###-

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

## Godfrey, Rob

**From:** Thad Westbrook <thad.westbrook@nelsonmullins.com>
**Sent:** Monday, October 29, 2012 2:41 PM
**To:** Godfrey, Rob
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

Thanks. I just spoke to Experian about this issue. They are investigating and addressing the issue right now.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 2:26 PM
**To:** Thad Westbrook
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

From Senator Graham's spokesman:

Bishop, Kevin (L. Graham)

Hey man, know you have million things going on right now. Just wanted to give you guys a heads up so you could let the credit people know about this issue with their website.

When you use Google Chrome browser it takes you to the page where you have to sign up to pay. I know people will get hacked getting that page after being told its free. I got that message.

When you use Internet Explorer it takes you to the correct page and allows you to use the Code you are providing.

Just FYI.

**From:** Thad Westbrook [mailto:thad.westbrook@nelsonmullins.com]
**Sent:** Monday, October 29, 2012 2:24 PM
**To:** Godfrey, Rob; Stirling, Bryan
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

I'm contacting Experian about this. There should be no charge.

**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 1:58 PM
**To:** Stirling, Bryan; Thad Westbrook
**Subject:** FW: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

**From:** Klump, Allen [mailto:Allen.Klump@mail.house.gov]
**Sent:** Monday, October 29, 2012 1:55 PM
**To:** Godfrey, Rob
**Subject:** RE: Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

FYI, I just did this and it made me pay $3 for my credit report

Allen G. Klump
Communications Director
The Office of Congressman Jeff Duncan SC-3
303 West Beltline Blvd.
Anderson, SC 29625
Cell: 864-915-4059



**From:** Godfrey, Rob [mailto:RobGodfrey@gov.sc.gov]
**Sent:** Monday, October 29, 2012 1:22 PM
**Subject:** Video: Gov. Nikki Haley, SLED Chief Mark Keel update taxpayers, media on DOR information security breach

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

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

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

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

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

- For any South Carolina taxpayer residing in South Carolina who wishes to bypass the telephone option, there currently is an online service available at http://www.protectmyid.com/scdor. Enter the code **SCDOR123** when prompted. Every South Carolina taxpayer who takes the time to sign up will be afforded the protection, and that protection is retroactive. South Carolina taxpayers have until the end of January, 2013 to sign up. South Carolina taxpayers who sign up for protection will be notified about how to sign up for a "Family Secure

Plan" if they claim minors as dependents.

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

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

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

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

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

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

-###-

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