Pitts, Ted

From: Harry Cooper <COOPERH@sctax.org>
Sent: Friday, January 18, 2013 2:58 PM
To: Pitts, Ted; Bill Blume
Cc: Meredith Cleland; Godfrey, Rob
Subject: RE: WLTX Interview Request

Ted,

Sorry I wasn't available when your email came in. Once Bill called me, I followed up with Meredith and Samantha. We did the on-camera with WLTX at 1:00—it went well. Jennifer was pleased and we offered to do another interview with her this Tuesday—she seemed happy.

I've also followed up with Meredith and Samantha on how something like this could happen. Here is her explanation:

DOR was first contacted this week through an email from WLTX's Nate Stewart where they asked for a statement on electronic filing. We provided a statement that was related to the security of electronic filing. A different reporter from WLTX, Jasmine, called at approximately the same time asking for an interview regarding filing safeguards since she was taking over the story. Samantha called Jasmine and offered to do an interview at the beginning of next week at the time, we plan to put out a press release about the new fraudulent refund program. Samantha also offered to answer any questions that Jasmine may have. Jasmine sent questions related to filing to which Samantha responded. Samantha stated that Jasmine was very friendly and cooperative and expressed no issues with the interview being at a later date. Subsequently, on Friday she got a call from a different reporter, Jennifer, who also asked for an interview. Samantha relayed the conversation with Jasmine and the plans for an interview next week. She then got an email from Sharranda stating that they would rather the interview take place today rather than early next week.
We then called Sharranda and she passed us on to Jennifer who we set up an interview with for 1 pm. We offered to also still do the interview next week at the time of the press release related to fraudulent refunds.
The interview today seemed to go well and Jennifer seemed pleased. We will be back in contact with Jennifer next week. Samantha always promptly responds to any media requests. In this particular case, she thought that with WLTX's apparent approval, they would benefit more from the beefier interview early next week where the fraudulent refund program could be revealed which was related to filing income tax returns.

I've advised Samantha that we must provide the reporters with what they are requesting in a timely fashion—not offer our own solutions. Meredith was asked to monitor Samantha closely and head off any similar incidents.

Again I am sorry this occurred and will also keep closer tabs on her activity.

Harry

From: Pitts, Ted [mailto:TedPitts@gov.sc.gov]
Sent: Friday, January 18, 2013 12:14 PM
To: Harry Cooper; Bill Blume
Cc: Meredith Cleland; Godfrey, Rob
Subject: FW: WLTX Interview Request

Harry,

See email from WLTX below.

DOR needs to get WLTX answers to some questions today by 4pm.

Nothing gets the Governor more upset than to see "the agency wouldn't respond to our multiple requests" in a story.

Please copy Rob on the response.

Ted

From: Godfrey, Rob
Sent: Friday, January 18, 2013 12:06 PM
To: Pitts, Ted
Subject: FW: WLTX Interview Request

From: Neal, Sharranda [mailto:sneal@wltx.gannett.com]
Sent: Friday, January 18, 2013 11:35 AM
To: cheeks@sctax.org
Cc: Godfrey, Rob; Bellamy, Jennifer
Subject: FW: WLTX Interview Request

Hi Samantha,
I hope you are well.
I'm following up on your correspondence with Jennifer Bellamy today.
I assigned her this story, and the other reporters earlier in the week, because we still haven't received adequate information to report to our viewers. Telling us you're releasing further information next week doesn't answer our questions. People are beginning to get their tax information in order for the filing season, and they want answers as to whether their information will be secure once filed and what changes have been made to ensure that security.
I'm sure I don't need to remind you of the impact this has had in our state. So, we would appreciate an on-camera interview—today—to help to allay some of these fears.
Please let me know who will be available and what time.
I'm copying Rob Godfrey at the Governor's Office on this email, because I'd like to keep them in the loop in the event that they have someone available to give us an on-camera interview as well. Rob, if that's a possibility—hearing from the Governor would be ideal.

We appreciate your help,

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

From: Samantha Cheek [mailto:CheekS@sctax.org]
Sent: Friday, January 18, 2013 11:27 AM
To: Bellamy, Jennifer
Subject: RE: WLTX Interview Request

Hi Jennifer,

Two other individuals from WLTX have already contacted me this week regarding this story: we plan to release further information on safeguards for income tax filing season at some point next week. During that time, I'd be happy to set up an interview with you to discuss filing season.

Thanks!

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

From: Bellamy, Jennifer [mailto:jbellamy@wltx.gannett.com]
Sent: Friday, January 18, 2013 10:35 AM
To: Samantha Cheek
Subject: WLTX Interview Request

Hello Samantha,

With tax season coming up, I wanted to put together a story for our viewers on filing their taxes electronically. I wanted to share some information on what the state may have done since the DOR hacking that might give them some confidence in filing electronically. I would like to do an on camera interview with someone from DOR about this today for a story to air in our shows this evening.

I also left a voicemail for you with this request as well.

Thanks in advance for your response,

Jennifer Bellamy
WLTX
Multimedia Journalist
(C) 803-309-9489
(O) 803-647-0247
Twitter: JBellamyWLTX
Facebook: Jennifer Bellamy WLTX

Pitts, Ted

From: Kim Jackson <KimJackson@schouse.gov>
Sent: Friday, January 18, 2013 3:13 PM
Subject: SCDOR Data Breach Investigative Committee Meeting - Thursday, January 24, 2013

MEMORANDUM

TO: The Honorable Harry Ott
The Honorable Shannon Erickson
The Honorable Laurie Slade Funderburk
The Honorable Dwight Loftis
The Honorable James Merrill
The Honorable Andy Patrick
The Honorable Ronnie Sabb
The Honorable Bakari Sellers
The Honorable Gary Simrill

FROM: The Honorable Bruce Bannister, Chairman

DATE: January 18, 2013

SUBJECT: **SCDOR Data Breach Investigative Committee Meeting**

The following meeting has been scheduled for the SCDOR Data Breach Investigative Committee:

Thursday, January, 24, 2013: 1 ½ hours after adjournment in Room 521 of the Blatt Building.

The committee will hear testimony about the Department of Revenue data breach and related security issues. Other items may be added.

cc: Ann Martin (5th Floor Receptionist - Blatt Building)
Sergeant at Arms (Mitch Dorman 2nd Floor State House)
Press Room (3rd Floor State House)
The Honorable Robert W. Harrell, Jr., Speaker of the House (506 Blatt Building)

Kim Jackson
Executive Secretary
South Carolina House of Representatives
Ways and Means Committee
803.734.3144 Telephone
803.734.2826 Fax
kimjackson@schouse.gov

Pitts, Ted

From: Rep. Bill Taylor <bill@taylorschouse.com>
Sent: Friday, November 02, 2012 3:11 PM
To: Pitts, Ted
Subject: HACKING - More FAQs from the Governor's Office

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

HACKING - More FAQs from the Governor's Office

(Friday Nov 2 - Informational Newsletter)

Dear Friends:

Questions continue to arrive in the aftermath of the S.C. hacking incident that put most of you at risk for fraud and identity theft. Your questions are sent to the Governor's office for answering. The Governor's staff and attorneys are providing answers. The following FAQ's just arrived from the Governor's office and I want you to have the information ASAP.

INDIVIDUAL TAXPAYER

Q: Who may have been affected by the SC DOR security breach?

A: Individual taxpayers, their dependents, and businesses who have filed a South Carolina tax return since 1998 to the present may have been affected.

Q: What type of personal information may have been exposed?

A: While the investigation is still ongoing, South Carolina taxpayer's Social Security Numbers, debit card numbers, credit card numbers, and information that would be found on the front of a check like bank account and routing numbers may have been exposed.

Q: What should you do if you have filed a SC tax return since 1998 to the present?

A: If you have filed a South Carolina tax return since 1998 to the present, the State is offering you the opportunity to register with ProtectMyID™ free of charge. There are two ways to register:

Option One: Sign up online.

- Go to www.protectmyid.com/scdor and use the activation code: SCDOR123 to initiate the registration process. All future notices from Experian® will be sent to you by email.
- Only one email address may be associated with one registration for ProtectMyID™.

Option Two: Call the Experian® Call Center.

- Call 1-866-578-5422 to complete the process with a live agent. You may choose to have all future notices from Experian® sent to you by postal mail or email.

If a taxpayer has no access to the internet, does not have a working email address, or if there is another reason why he or she cannot access the internet, then he or she must call the Experian® Call Center.

Q: What are the hours of operation for the Experian® Call Center?

A: Monday - Friday: 9:00 a.m. - 9:00 p.m. EST
Saturday and Sunday: 11:00 a.m. - 8:00 p.m. EST

Q: What benefits will a taxpayer receive after registering with ProtectMyID™?

A: Experian® will provide the following:

- Credit Report: You will get a free copy of your Experian® credit report.
- Daily Credit Monitoring: You will receive alerts regarding any suspicious activity, including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian®, Equifax® and TransUnion® credit reports for one year.
- 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.
- Identity Theft Insurance: If you have been a victim of identity theft, you will immediately be 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 for one year.
- ExtendCARE: You will get full access to personalized assistance from a highly-trained Fraud Resolution Agent even after the initial one year ProtectMyID™ membership expires.

Q: Is there a deadline to register with ProtectMyID™?

A: January 31, 2013 is the deadline to register for one year of identity theft protection with ProtectMyID™.

Q: How much does it cost to register with ProtectMyID™?

A: No fee is charged to the enrollee to register with ProtectMyID™ for the first year.

Q: How will someone be contacted who has filed a tax return since 1998 to the present in SC and no longer lives in the state?

A: Notice will be sent to them by standard U.S. mail.

CHILDREN: MINORS / DEPENDENTS / Family Secure™ COVERAGE

Even though your minor dependent may not have a credit history, you may enroll them for identify theft protection. All individuals under the age of 18 must be enrolled by one parent or guardian. A parent or guardian will be notified several weeks after registration when Family Secure™ enrollment has opened by postal mail or email.

- Minors are individuals under the age of 18.
- Dependents are individuals who are claimed as dependents for tax filing purposes.

Q: Have minors' Social Security Numbers been exposed?

A: Social Security Numbers of minors and/or dependents may have been exposed.

Q: How do I enroll a minor for Family Secure™ coverage?

A: There are 3 steps to follow:

- Step One: A minor's parent or guardian must first enroll with ProtectMyID™. Only one parent or guardian may enroll the minor.
- Step Two: The parent or guardian, who enrolled in ProtectMyID™, will receive a letter or email explaining how to enroll minor dependents in the Family Secure™ plan.
- Step Three: The parent or guardian, who enrolled in ProtectMyID™, will then enroll minor dependents in the Family Secure™ plan.

Q: After being enrolled as a minor in the Family Secure™ plan, what should I do when I turn 18 years old or begin to file tax returns?

A: Call Experian® for assistance 1-866-578-5422.

Q: What are the benefits of Family Secure™ coverage?

A: The primary benefit that Family Secure™ offers is monitoring the identity (primarily the SSN) of the minor for one year, even if the minor has no credit report. Once registered, in the event a child does not have a credit file, if any credit, loan or similar account is opened with that information, Experian® will alert the parent or guardian. Details of the alerts on minors are not released unless or until the parent or guardian authenticates themselves with Experian® as the parent or guardian of the minor.

Family Secure™ coverage is for one adult and any number of minors. (Five minors can be enrolled via the website. For more than five, the customer must call Experian®). The adult coverage includes a $2 million product guarantee covering the whole family, Score Tracker and Fraud Resolution.

Minors receive monthly monitoring for existence of a minor's credit report, and if a credit report is found, then Experian® monitors for any changes to that report.

Q: What if I file joint tax returns or have joint banking and credit accounts with my spouse?

A: Every individual with a Social Security Number should register with ProtectMyID™ separately, because credit histories are tied to individual's Social Security Numbers.

Q: Will my deceased family members be at risk?

A: It is not necessary to sign the deceased up for ProtectMyID. However, you should notify all three credit bureaus (Experian®, Equifax® and TransUnion®).

ADULT DEPENDENT / DISABLED

Q: How do I protect an adult who is a dependent and/or is disabled?

A: The individual charged with the legal authority to assist a dependent adult filing taxes can enroll the dependent adult with ProtectMyID™ as long as that individual provides proper documentation to Experian®.

MILITARY PERSONNEL

Q: What if I serve in the military and filed taxes in South Carolina since 1998 to the present?

A: The State of South Carolina will work with the U.S. Department of Defense to identify and notify all military personnel who have filed South Carolina taxes since 1998 to the present.

BUSINESSES

Q: What should I do if I am a business owner?

A: South Carolina business owners are being offered two free products. Businesses have the opportunity to enroll with both Dun & Bradstreet and Experian® Business Credit AdvantageSM.

Q: What type of business information may have been exposed?

A: While the investigation is still ongoing, Federal EIN numbers, SC Department of Revenue tax ID numbers, credit and debit card information, and bank account information may have been exposed.

Dun & Bradstreet:

If your business has filed a South Carolina tax return since 1998, you should contact Dun & Bradstreet Credibility Corp. who will give South Carolina businesses a CreditAlert product that will help them stay alerted to changes in their D&B® scores or ratings and other indicators of fraudulent activity that could be taking place on their business. The deadline to register with Dun & Bradstreet is January 31, 2013. There are two ways to register:

Option One: Sign up online.

- Go to visit www.DandB.com/SC to initiate the registration process.

Option Two: Call Dun & Bradstreet Credibility Corp. Call Center.

- Call 1-800-279-9881 to complete the process with a live agent.
- Hours of Operations: Monday - Friday: 8:00 a.m. -8:00 p.m. EST.

Experian® Business Credit AdvantageSM:

If your business filed a South Carolina tax return since 1998, Experian® is offering a comprehensive business credit monitoring service called Business Credit AdvantageSM - a service that allows unlimited access to the company's complete business credit report and score, plus instant email notifications of changes to the business credit profile. These email alerts include reported changes to the business address, credit inquiries, newly opened credit lines, and score changes. South Carolina businesses can begin to view and protect their business credit information with Experian® by signing up for Business Credit AdvantageSM at www.smartbusinessreports.com/SouthCarolina.

How-to-enroll:

1.) Go to www.SmartBusinessReports.com/SouthCarolina
2.) Register to get an Experian® business credit monitoring access code
3.) An instant email is sent to the user's email address with the access code
4.) Follow instructions on the email to redeem the access code at the web address provided

---

Our Apology

It is believed this incident was caused by an organization of international cyber hackers. The situation is most regrettable for it puts each of you at risk for fraud and identity theft, as well as placing a burden on everyone to take personal actions to safeguard themselves and their accounts from crooks. On behalf of the State of South Carolina, please accept our sincerest apology for this aggravation and inconvenience.

Extending Your Protection

Personally, I do not believe one year of credit monitoring is sufficient. It's understandable that the one year period was negotiated as a quick fix to an immediate crisis. But crooks are patient, so you need a longer period for free credit monitoring. **When we return to Columbia for the next legislative session, I will join other representatives in exploring ways to extend the period for**

credit protection monitoring.

In your Service,

Bill Taylor
803-270-2012
Representative
South Carolina General
Assembly
Bill@taylorschouse.com
www.Taylorschouse.com

Newsletter not paid for by
taxpayer funds.

Paid for by TaylorSCHouse

This email was sent to tedpitts@gov.sc.gov by bill@taylorschouse.com |
Update Profile/Email Address | Instant removal with SafeUnsubscribe™ | Privacy Policy.
Bill Taylor for SC House District 86 | P.O. Box 2646 | Aiken | SC | 29801

Pitts, Ted

From: Debbie Barthe <DebbieBarthe@scsenate.gov>
Sent: Friday, November 02, 2012 1:51 PM
To: Pitts, Ted
Subject: FW: DOR SS# Info Hacked ~ Website email from Larry Ward

Mr. Pitts,

Senator Davis ask that I refer Mr. Ward to your attention.

Larry [redacted]
[redacted]
Bluffton, SC 29909

843[redacted]

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Friday, November 02, 2012 1:10 PM
To: Debbie Barthe
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

This is for the one year coverage. My concern is after that.

From: DebbieBarthe@scsenate.gov
To: [redacted]@msn.com
Date: Fri, 2 Nov 2012 11:52:53 -0400
Subject: FW: DOR SS# Info Hacked ~ Website email from Larry[redacted]

Also attached is some information we received from the Gov. office this morning.

Debbie Barthe
For Senator Tom Davis

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Friday, November 02, 2012 11:36 AM
To: Tom Davis
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry[redacted]

Thank you.

From: TomDavis@scsenate.gov
To: [redacted]@msn.com
Date: Fri, 2 Nov 2012 11:23:51 -0400
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry[redacted]

Mr. Ward,

Senator Davis is reviewing your email. In the meantime, here is some information I found on the Experian website which may address your questions about the $1 Million Identity Theft Insurance and credit fraud resolution.
Debbie Barthe
For Senator Tom Davis

All ProtectMyID members receive $1 Million Insurance with zero deductible the minute they enroll. This means that if you become a victim of identity theft while you are a member you may be covered for any of the following:

- - Illegal Electronic Fund Transfers (EFT)
- - Lost Wages
- - Private Investigator Costs
- - Legal Defense Fees
- - And much more

Once you have filed a fraud resolution case with our Identity Theft Resolution Agents, we will immediately work with you on resolving identity fraud. Our Agents will help you contact the proper authorities and assist in the paperwork.
Our identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. View Summary of Benefits.

Summary Description of Benefits for the Experian Identity Theft Coverage

This Summary Description of Benefits (the "Summary") is provided to inform you that as a member of ProtectMyID™ you are entitled benefits under the Master Policy referenced below. This Summary does not state all the terms, conditions, and exclusions of the Master Policy. Your benefits will be subject to all of the terms, conditions, and exclusions of the Master Policy, even if they are not mentioned in this Summary. A complete copy of the Master Policy will be provided upon request.
The Master Policy of Fraud Safeguard Coverage for New York Insureds and the Master Policy of Personal Internet Identity Coverage for non-New York Insureds (collectively, the "Master Policy") have been issued to ConsumerInfo.com, Inc. (the "Master Policyholder"), under Policy Numbers: [1423382 and 7077868, respectively underwritten by insurance company subsidiaries or affiliates of Chartis Inc., to provide benefits as described in this Summary.

GENERAL INFORMATION

Should you have any questions regarding the Membership Program provided by the Master Policyholder, or wish to view a complete copy of the Master Policy, please call the customer service number located in your membership materials.
Limit of Insurance

Aggregate Limit of Insurance for each Child Secure Program:	$ 2,000,000
Aggregate Limit of Insurance for each insured (other than an insured enrolled in the Child Secure Program):	$ 1,000,000
Lost Wages:	$ 1000 per week, for 4 weeks maximum
Deductible	$ 0 per policy period

Reporting a Claim
To report a claim under the Master Policy, contact the Master Policyholder's Fraud Resolution Unit at 866-960-6943.
If the Master Policy is terminated, your benefits will cease effective the date of such termination. It is the obligation of the Master Policyholder to inform you of any termination of the Master Policy.

BENEFITS

- We shall pay you for the following in the event of a Stolen Identity Event:

    1. Costs

        1. Costs incurred by you for re-filing applications for loans, grants, other credit or debt instruments that are rejected solely because the lender received from any source incorrect information as a result of a Stolen Identity Event;
        2. Costs for notarizing affidavits or other similar documents, long distance telephone calls, and postage reasonably incurred as a result of your efforts to report a stolen identity event or amend or rectify records as to your true name or identity as a result of a stolen identity event; and
        3. Costs incurred by you for a maximum of six (6) credit reports from an entity approved by us. The first credit report may not be requested until after the discovery of a stolen identity event;

    2. Lost Wages

        Actual lost wages that would have been earned in the United States, its territories or possessions, whether partial or whole days, for time reasonably and necessarily taken off work and away from your work premises solely as a result of your efforts to amend or rectify records as to your true name or identity as a result of a Stolen Identity Event. Actual lost wages includes remuneration for vacation days, discretionary days, floating holidays, and paid personal days.
        Lost wage reimbursement excludes business interruption or future earning of a self-employed professional. Computation of lost wages for self-employed professionals must be supported by and will be based on prior year tax returns.
        Coverage is limited to wages lost within twelve (12) months after your discovery of a Stolen Identity Event.

    3. Investigative Agency or Private Investigator Costs

        Costs associated with the use of any investigative agency or private investigator engaged to amend or rectify records as to your true name or identity as a result of a Stolen Identity Event. We reserve the right to select such investigative agency or private investigator; however, with our express prior written consent, you may select such investigative agency or private investigator.

    4. Legal defense fees and expenses

        Costs for reasonable fees for an attorney appointed by us and related court fees, incurred by you with our consent, for:

        1. Any legal action brought against you by a creditor or collection agency or entity acting on behalf of a creditor for non-payment of goods or services or default on a loan as a result of a Stolen Identity Event; and
        2. Removing any civil judgment wrongfully entered against you as a result of the Stolen Identity Event.
        3. Criminal defense for charges brought against you as a result of a Stolen Identity Event. However, we will only pay for this after it has been established by acquittal or dropping of charges because you were not in fact the perpetrator.

        A Stolen Identity Event is the fraudulent use of your personal identification, social security number, or other method of identifying you, including the fraudulent use of your personal identity to establish credit accounts, secure loans, enter into contracts or commit crimes. A Stolen Identity Event does not include the theft or unauthorized or illegal use of your business name, d/b/a or any other method of identifying your business activity.

- We shall pay you for the following in the event of an Unauthorized Electronic Fund Transfer:

1. The principal amount, exclusive of interest, incurred by you and caused by an Unauthorized Electronic Fund Transfer first occurring during the policy period. However, such principal amount shall not include any amount for which you did not seek reimbursement from the financial institution which issued the access device and holds the account from which funds were stolen, and for which you have not received reimbursement from any other source.
   An Unauthorized Electronic Fund Transfer (UEFT) is an electronic fund transfer from your Account initiated by a person other than you without the actual authority to initiate such transfer and from which you receive no benefit. An Unauthorized Electronic Fund Transfer (UEFT) does not include an electronic fund transfer initiated: 1) by a person who was furnished the access device to your account by you, unless you have notified the financial institution that transfers by such person are no longer authorized; 2) with fraudulent intent by you or any person acting in concert with you; 3) by the financial institution of its employee; or 4) from any business or commercial account.
   Account means a cash, credit card, demand deposit (checking), savings or money market account of yours held directly or indirectly by a financial institution and established primarily for personal, family or household purposes.

COVERAGE SCOPE

Subject to the Master Policy´s terms, conditions and exclusions, the Master Policy provides benefits to you only if: (1) you report a Stolen Identity Event or an Unauthorized Electronic Fund Transfer to the Master Policyholder at the contact number stated above as soon as you become aware of a Stolen Identity Event or a Unauthorized Electronic Fund Transfer, but in no event later than ninety (90) days after the Stolen Identity Event or Unauthorized Electronic Fund Transfer is discovered; and (2) you follow the instructions given to you by the Fraud Resolution Unit. These instructions will include notifying major credit bureaus, the Federal Trade Commission's Identity Theft Hotline and appropriate law enforcement authorities. You will also be provided with a claim form and instructed how to file for benefits under the policy if the Stolen Identity Event or Unauthorized Electronic Fund Transfer results in losses covered under the policy.
You will only be covered for a Stolen Identity Event if a Stolen Identity Event is first discovered while you are a member of the Master Policyholder´s insured program and is reported to us within ninety (90) days of such discovery.
You will only be covered for an Unauthorized Electronic Fund Transfer if an Unauthorized Electronic Fund Transfer first occurs while you are a member of the Master Policyholder´s insured program and is reported to us within ninety (90) days of such discovery.
You will not be covered if the Stolen Identity Event or Unauthorized Electronic Fund Transfer first occurs after termination of the master policy or termination of your membership in the Master Policyholder´s program.

LIMITS OF INSURANCE

The most we shall pay you are the Limits of Insurance shown above. All Legal Costs shall be part of and subject to the Aggregate Limit of Insurance. LEGAL COSTS ARE PART OF, AND NOT IN ADDITION TO, THE LIMIT OF INSURANCE.
Each aggregate sublimit of liability in this policy is the maximum limit of the Insurer´s liability for all loss under the policy that is subject to that aggregate sublimit of liability. All sublimits of liability shall be part of, and not in addition to, the Limit of Insurance.
The Lost Wages Limit of Insurance shown above is a sublimit of the Aggregate Limit of Insurance and is the most we shall pay you for lost wages.

OTHER INSURANCE

We shall be excess over any other insurance, including, without limitation, homeowner´s or renter´s insurance. If you have other insurance that applies to a loss under this policy, the other insurance shall pay first. This policy applies to the amount of loss that is in excess of the Limit of Insurance of your other insurance and the total of all your deductibles and self-insured amounts under all such other insurance. In no event shall we pay more than our Limits of Insurance as shown above.

DUPLICATE COVERAGES

If you are enrolled in more than one Membership Program insured by us, or any of our affiliates, we will reimburse you under each membership program:

a) subject to the applicable deductibles and Limits of Insurance of each insured Membership Program
b) but in no event shall the total amount reimbursed to you under all Membership Programs exceed the actual amount of loss.

From: Larry [redacted] [mailto:larryw0320@msn.com]
Sent: Friday, November 02, 2012 8:46 AM
To: Tom Davis
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry Ward

Thanks for your reply Tom,

However, this doesn't help the taxpayers that are or will be effected by this irresponsible action by the State of South Carolina.

1) I don't trust the governor, by the way she has handled this. It should have been disclosed earlier instead of a Friday afternoon news dump. The governor said that leaving Social Security numbers unencrypted is a common industry practice due to the complicated nature of the encryption process. T**his is not true.**

2) The State is going to provide monitoring for 1 year, so I assume the tax payer will be have to pay after the one year, which in some cases of children having their SS#, etc. listed on their parent's tax returns could go on for 70+ years. at $19.95 a month each.

3) No one has explain what Credit Fraud Resolution for life is. Does it mean if my SS# is used fraudently by a thief, that the State will be responsible for the necessary action to correct this theft? How long will it take? I am sure you have heard the horror stories.

Larry[redacted]

From: TomDavis@scsenate.gov
To: [redacted]@msn.com
Date: Thu, 1 Nov 2012 12:07:24 -0400
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Dear Larry,

Like you, I was shocked last Friday to learn that computer systems at the S.C. Department of Revenue had been breached on numerous occasions, and that 3.6 million Social Security numbers and nearly 400,000 credit and debit card numbers had been obtained by what the governor's office has called "an international hacker." And I was stunned again yesterday when the governor announced the data of more than 650,000 businesses was also part of the hack.

For the past several days, I have communicated with the offices of Gov. Nikki Haley, SLED Chief Mark Keel, State Department of Revenue Director Jim Etter and others to learn more about this security breach. Obviously, state government has failed the people of South Carolina, and I pledge to you that an exhaustive inquiry will be conducted, that those guilty of malfeasance will be identified, and that appropriate steps will be taken to ensure that such sensitive information provided by citizens to their government is better protected in the future.

Tough questions will be asked and answers demanded. Questions such as: Why wasn't the credit card data kept in an unencrypted format? Was the breach the result of human error or inadequate security procedures? Why was data kept in a way that was accessible to the internet? What is the security audit process and how often is it conducted? What was the reason for the delay in advising the public of the security breach?

At this point, though, it is more productive to focus on how taxpayers can protect themselves, and to answer the most frequently asked questions. The information listed below in Q&A format has been provided by the governor's office, by Experian (the credit-protection agency retained by the governor's office), or by state newspapers who have assigned their best investigative reporters to uncover the facts. (In that latter regard, particular thanks are owed to The Greenville News; much of what is listed below can be found on its website.)

The governor's office provides regular updates on this situation, as do newspapers and other news outlets, and I post that information on my Facebook page and website as it becomes available. I invite you to visit https://www.facebook.com/senatortomdavis and/or www.senatortomdavis.com for that additional information.

Q: What steps do I need to take to protect my identity?

A: The governor and SLED chief said they do not know exactly what information was stolen, but they are urging anyone who filed a South Carolina tax return since 1998 to sign up for Experian's ProtectMyID service by calling 1-866-578-5422 or visiting the web site at protectmyid.com/scdor and using the activation code SCDOR123. The governor has said that the state will provide those affected with one year of credit monitoring and identify-theft protection.

Q: Are young adults that previously filed in SC covered by the consumer protection service?

A: If a tax return was filed from 1998 until present and a person's social security number 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.

Q: Do South Carolina residents need to do anything other than sign up with Experian to be fully protected?

A: In addition to the Experian product, state officials urge 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.

Q: If a South Carolina resident called and got a user name and password before the SCDOR123 code was announced, are they protected?

A: Yes.

Q: Do people have to call or can they do sign up online without calling?

A: If people have the signup code, they can go directly online to enroll. People are not required to call first. There are still people unaware of the online registration option and the call serves as the best means to inform them of that option.

Q: What about other credit reporting agencies? Do people need to sign up with them, or is that purely redundant?

A: Experian's ProtectMyID Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus.

Q: What's the process for enrolling minor children in ProtectMyID?

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

Q: What are the requirements for getting my child covered under Family Secure?

A: Individuals must sign up for ProtectMyID first. Once they are registered, notification and a registration code (different from the one used for ProtectMyID) will be sent to them, with directions what to do to register minors with Family Secure. Those who registered online will receive this notification via email. Those who registered over the phone will receive the notification in the mail. This process will take two to three weeks. If you do not have minors listed as

dependents, you can ignore the notice if you receive it. As with ProtectMyID, the Family Secure registration process may be completed via the phone with a live representative or online. Parents register their children as part of Family Secure.

Q: What are the benefits of Family Secure?

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

Family Secure coverage is for one adult and any number of minors. (Five minors can be enrolled via the website. For more than five, the customer must call Customer Care). The adult coverage includes a $2 million product guarantee covering the whole family, Score Tracker and Fraud Resolution.

Minors receive monthly monitoring for existence of a minor's credit report, and if a credit report is found, then we monitor for any changes to that report.

Q: How do I enroll my children in the identity theft protection plan?

A: The governor said during Tuesday morning's update that once you are signed up with Experian you will be notified by the company about enrolling minors in your family who have been associated to your Social Security number. According to the governor, if you are eligible to receive a family plan, the notification will arrive via e-mail if you signed up for the service online or a mailed letter if you signed up by calling the toll-free line.

Q: What period of time will this protection cover?

A: The governor said that those who sign up will be covered retroactively and they have until the end of January to get enrolled. Under a deal negotiated with Experian, South Carolina citizens whose tax returns were hacked will be eligible for credit fraud resolution for life, according to officials.

Q: What if I don't own a computer or have Internet access? Can I still enroll in the identity protection program?

A: Yes. Call 1-866-578-5422 to get assistance with enrollment over the phone. The governor said Tuesday that wait times averaged 10 minutes and that it took about nine minutes to get signed up once you get through.

Q: Why do I have to sign myself up? Why doesn't the state automatically sign the 3.6 million individuals potentially affected by the cyber hacking incident up for identity protection services?

A: The governor said that the state is not legally permitted to sign individuals up for a service in which they may not desire to participate.

Q: How much is this costing the state?

A: The governor said Tuesday morning that the state and Experian have agreed to cap security costs to the state at $12 million.

Q: Has the cyber hacker been identified or apprehended?

A: The SLED chief said no arrests have been made. Law enforcement officials have declined to answer specific questions about the investigation, describing it as "sensitive" and "complex."

Q: What exactly was taken?

A: The governor and SLED chief have said 3.6 million social security numbers and 387,000 mostly encrypted credit and debit card numbers were exposed, and that the data of more than 650,000 businesses was also part of the hack. Officials said they don't yet know how many of the numbers were actually taken, but said the scope of the breach includes anyone who has filed a South Carolina tax return since 1998.

Q: When did it happen?

A: The breach, the result of four intrusions into Revenue Department computers that began August 27 and continued until September 13, was discovered October 10. A Secret Service agent said the agency's computer crimes office first uncovered the intrusion and notified state authorities. The attack was not disclosed to the public until last Friday (September 26).

Q: Why wasn't the stolen information encrypted?

A: The governor said that leaving Social Security numbers unencrypted is a common industry practice due to the complicated nature of the encryption process. Some in the credit-security industry say encryption technology is readily available for data stores and is not cumbersome. Regardless, going forward, such data in South Carolina will be encrypted.

Q: Are other state agencies vulnerable to cyber hacking? Does other personal information remain at risk?

A: The governor asserted in a press conference that any agency, state or federal, can be hacked.

Tom Davis
Senator, Beaufort County
Senate District 46

Columbia Office:
P.O. Box 142
602 Gressette Building
Columbia, SC 29202
Tel: 202-212-6008 - Fax: 803-212-6299
Senate EMAIL: tomdavis@scsenate.gov

Beaufort Ofice:
Post Office Drawer 1107
1001 Craven Street
Beaufort, SC 29901-1107
Tel: 843-252-8583- Fax: 843-524-6401
District EMAIL: tom@senatortomdavis.com

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Thursday, November 01, 2012 9:38 AM
To: Tom Davis
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

This thing just keeps getting better!!!

Now we are told business information was stolen and they get treatment than individuals.

Like other S.C. taxpayers, state businesses will be able to get free credit monitoring. But companies will get longer coverage.
Businesses that have filed state taxes since 1998 can sign up for lifetime record monitoring from Experian starting today and Dun & Bradstreet starting Friday. Consumers can get one year of monitoring and insurance from Experian, paid for by the state. However, individual taxpayers will have to pay to continue the coverage after one year. Consumers will get lifetime credit-fraud resolution as

part of Experian's agreement. The cost to the state for those services has been capped at $12 million.

Read more here: http://www.thestate.com/2012/11/01/2503354/657000-sc-business-records-also.html#storylink=cpy

I received a email back from the Director of Revenue CIO, thanks alot, basically giving me the same spin.

I asked her what lifetime credit-fraud resolution was and have heard nothing back.

Thanks

Larry Ward

From: TomDavis@scsenate.gov
To: [redacted]@msn.com
Date: Tue, 30 Oct 2012 14:38:38 -0400
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Senator Davis is currently reviewing the emails he has received from folks in his district concerning the security breach at SC DOR. In the meantime, I thought you may be interested in reviewing his comments in the recent Island Packet article. He has been monitoring and following this situation closely. Please let us know if you have any further information to share with our office.

Debbie Barthe
Office of Senator Tom Davis
Gressette Building 602
P.O. Box 142
Columbia, SC 29202
Phone: 803-212-6008
Fax: 803-212-6011
E-Mail: debbiebarthe@scsenate.gov

From: [redacted]@msn.com [mailto:[redacted]@[redacted]]
Sent: Monday, October 29, 2012 9:54 AM
Subject: DOR SS# Info Hacked ~ Website email from Larry[redacted]

I am very upset about this! Why wasn't the Citizens informed when it happened in August? Why wasn't this information protected? What is being done to take care of this? SECURITY COMPROMISED SC officials plan on hacking update Monday morning Cyber-hacked SC taxpayers frustrated with help tips from state officials By CLIF LeBLANC - cleblanc@thestate.com E-MAIL PRINT REPRINT 57 COMMENTS TEXT SIZE: COLUMBIA, SC - Correction: The S.C. Consumer Affairs Department number is (800) 922-1594. As some South Carolina taxpayers, fearing their tax records have been hacked, complain about difficulties in getting access to the state's newly created self-help system, state leaders plan a Monday morning update on the massive security breach. Gov. Nikki Haley and SLED Chief Mark Keel have scheduled a 10.a.m. news conference at the State House. But an announcement from Haley%u2019s spokesman Rob Godfrey gives no indication of which aspects for the invasion of privacy case they plan to address. Video from around the

world The governor%u2019s office also had scheduled a conference call at the same time for legislators. Godfrey said Sunday they will adjust the briefing to either just before or just after the news conference. Haley, Keel and other state and federal authorities on Friday disclosed that a foreign hacker or hackers had stolen 3.6 million Social Security numbers and 387,000 credit or debit card numbers from the S.C. Department of Revenue during a series of cyber attacks that date to Aug. 27. None of the data - except 16,000 of the credit card numbers %u2013 was encrypted, Revenue Department director James Etter said. State officials advised anyone who had filed a state tax return since 1998 to take steps to learn if their information had been misused by identity thieves. The state laid out procedures that worried taxpayers should take to determine if their information was misused and/or to protect themselves: Call (866) 578-5422, a hot line, to be given an access code to a website where they could register for one year of free credit monitoring. %u2022 A recording at the phone number provides a standard activation code (SCDOR123) that can be used at a web address: www.protectmyID.com/scdor. %u2022 The Revenue Department said it would have more receptionists at its call center over the weekend to help with the flood of calls. %u2022 The S.C. Consumer Affairs Department planned to add part-time staffers to answer phone calls during business hours starting today. Call (800) 922-1594 for advice or to request a freeze on your credit records. Privacy advocates say that is the surest way to block identity theft. Despite those steps, many South Carolinians were frustrated with the state%u2019s response over the weekend. Many emailed or called The State newspaper and other media outlets to vent, though some said they were given assistance through the hot line and the website. One woman complained she had trouble getting through to the web address that state officials provided. She decided to spend $35 to get a credit report to see if there was any unauthorized activity. A man said he got repeated recorded messages at the hot line and the web address was recited too quickly for him to write it down. He wrote the newspaper saying that his biggest worry remains: "whether or not I am one of whose records were stolen." Godfrey said Sunday that more people manned phone banks as soon as state officials learned of the phone delays. %u201CAnd the number of representatives has continued to increase over the weekend.%u201D By releasing the access code publicly, taxpayers should be able to speed the process of seeking credit protection, Godfrey said. %u201CIf we need to take any further action to make sure our taxpayers are protected, we will do so %u2013 and do so swiftly,%u201D the spokesman said. Read more here: http://www.thestate.com/2012/10/28/2499098/sc-officials-plan-on-hacking-monday.html#storylink=cpy

Larry [redacted]
[redacted]
Bluffton, SC 29909
843[redacted]

Pitts, Ted

From: Tom Davis <TomDavis@scsenate.gov>
Sent: Monday, November 05, 2012 9:45 AM
To: Pitts, Ted; Veldran, Katherine
Subject: FW: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Katherine,

Could you guys please speak with Mr. [redacted] directly on his concerns? See email strings below.

Debbie Barthe
For Senator Tom Davis

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Monday, November 05, 2012 9:24 AM
To: Debbie Barthe
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry Ward

So I guess the taxpayer is on the hook for trying to get his Identity Theft resolved. The Taxpayer will be walked through the fraud resolution process from start to finish.
THIS CAN TAKE FOREVER, WHY DOES THE TAXPAYER HAVE TO RESOLVE THIS PROBLEM, WHY NOT THE STATE SINCE THEY ARE THE ONES AT FAULT.

How is the state going to resolve Stolen Identities that have been used in thefts, fraud and other criminal actions? IRS issues?

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.
• Identity Theft Insurance: If you have been a victim of identity theft, you will immediately be 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 for one year.

From: DebbieBarthe@scsenate.gov
To: [redacted]@msn.com
Date: Mon, 5 Nov 2012 09:04:40 -0500
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Mr. [redacted]

This was included in the latest update we received from the Governor's Office which was released to us on November 2, 2012. I have copied some of the information for your review and have attached the entire update for you also.
Thanks.

Debbie Barthe
For Senator Tom Davis

: How will someone be contacted who has filed a tax return since 1998 to the present in SC and no longer lives in the state?

A: Notice will be sent to them by standard U.S. mail.

Q: What benefits will a taxpayer receive after registering with ProtectMyID™?

A: Experian® will provide the following:

- Credit Report: You will get a free copy of your Experian® credit report.
- Daily Credit Monitoring: You will receive alerts regarding any suspicious activity, including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian®, Equifax® and TransUnion® credit reports for one year.
- 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.
- Identity Theft Insurance: If you have been a victim of identity theft, you will immediately be 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 for one year.
- ExtendCARE: You will get full access to personalized assistance from a highly-trained Fraud Resolution Agent even after the initial one year ProtectMyID™ membership expires.

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Monday, November 05, 2012 8:44 AM
To: Debbie Barthe
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Tom,

Another problem I found over the weekend, when asking several people about this. They had not heard anything about it. One was a taxpayer who lives in Ga, but had worked in SC for a couple of years.

Shouldn't the State send out written notices to all taxpayers affected by this.

Also, I see where our esteem Governor is still only going to pay for 1 year of monitoring and then the taxpayers are on their on.

Larry [redacted]

From: DebbieBarthe@scsenate.gov
To:[redacted]@msn.com
Date: Fri, 2 Nov 2012 11:52:53 -0400
Subject: FW: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Also attached is some information we received from the Gov. office this morning.

Debbie Barthe
For Senator Tom Davis

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Friday, November 02, 2012 11:36 AM
To: Tom Davis
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Thank you.

From: TomDavis@scsenate.gov
To: [redacted]@msn.com
Date: Fri, 2 Nov 2012 11:23:51 -0400
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry Ward

Mr. [redacted]

Senator Davis is reviewing your email. In the meantime, here is some information I found on the Experian website which may address your questions about the $1 Million Identity Theft Insurance and credit fraud resolution.
Debbie Barthe
For Senator Tom Davis

All ProtectMyID members receive $1 Million Insurance with zero deductible the minute they enroll. This means that if you become a victim of identity theft while you are a member you may be covered for any of the following:

- - Illegal Electronic Fund Transfers (EFT)
- - Lost Wages
- - Private Investigator Costs
- - Legal Defense Fees
- - And much more

Once you have filed a fraud resolution case with our Identity Theft Resolution Agents, we will immediately work with you on resolving identity fraud. Our Agents will help you contact the proper authorities and assist in the paperwork.
Our identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. View Summary of Benefits.

Summary Description of Benefits for the Experian Identity Theft Coverage

This Summary Description of Benefits (the "Summary") is provided to inform you that as a member of ProtectMyID™ you are entitled benefits under the Master Policy referenced below. This Summary does not state all the terms, conditions, and exclusions of the Master Policy. Your benefits will be subject to all of the terms, conditions, and exclusions of the Master Policy, even if they are not mentioned in this Summary. A complete copy of the Master Policy will be provided upon request.
The Master Policy of Fraud Safeguard Coverage for New York Insureds and the Master Policy of Personal Internet Identity Coverage for non-New York Insureds (collectively, the "Master Policy") have been issued to ConsumerInfo.com, Inc. (the "Master Policyholder"), under Policy Numbers: [1423382 and 7077868, respectively underwritten by insurance company subsidiaries or affiliates of Chartis Inc., to provide benefits as described in this Summary.

GENERAL INFORMATION

Should you have any questions regarding the Membership Program provided by the Master Policyholder, or wish to view a complete copy of the Master Policy, please call the customer service number located in your membership materials.
Limit of Insurance

Aggregate Limit of Insurance for each Child Secure Program:	$ 2,000,000
Aggregate Limit of Insurance for each insured (other than an insured enrolled in the Child Secure Program):	$ 1,000,000
Lost Wages:	$ 1000 per week, for 4 weeks maximum

Deductible $ 0 per policy period

Reporting a Claim
To report a claim under the Master Policy, contact the Master Policyholder's Fraud Resolution Unit at 866-960-6943.
If the Master Policy is terminated, your benefits will cease effective the date of such termination. It is the obligation of the Master Policyholder to inform you of any termination of the Master Policy.

BENEFITS

- We shall pay you for the following in the event of a Stolen Identity Event:

1. Costs

    1. Costs incurred by you for re-filing applications for loans, grants, other credit or debt instruments that are rejected solely because the lender received from any source incorrect information as a result of a Stolen Identity Event;
    2. Costs for notarizing affidavits or other similar documents, long distance telephone calls, and postage reasonably incurred as a result of your efforts to report a stolen identity event or amend or rectify records as to your true name or identity as a result of a stolen identity event; and
    3. Costs incurred by you for a maximum of six (6) credit reports from an entity approved by us. The first credit report may not be requested until after the discovery of a stolen identity event;

2. Lost Wages

    Actual lost wages that would have been earned in the United States, its territories or possessions, whether partial or whole days, for time reasonably and necessarily taken off work and away from your work premises solely as a result of your efforts to amend or rectify records as to your true name or identity as a result of a Stolen Identity Event. Actual lost wages includes remuneration for vacation days, discretionary days, floating holidays, and paid personal days.
    Lost wage reimbursement excludes business interruption or future earning of a self-employed professional. Computation of lost wages for self-employed professionals must be supported by and will be based on prior year tax returns.
    Coverage is limited to wages lost within twelve (12) months after your discovery of a Stolen Identity Event.

3. Investigative Agency or Private Investigator Costs

    Costs associated with the use of any investigative agency or private investigator engaged to amend or rectify records as to your true name or identity as a result of a Stolen Identity Event. We reserve the right to select such investigative agency or private investigator; however, with our express prior written consent, you may select such investigative agency or private investigator.

4. Legal defense fees and expenses

    Costs for reasonable fees for an attorney appointed by us and related court fees, incurred by you with our consent, for:

    1. Any legal action brought against you by a creditor or collection agency or entity acting on behalf of a creditor for non-payment of goods or services or default on a loan as a result of a Stolen Identity Event; and
    2. Removing any civil judgment wrongfully entered against you as a result of the Stolen Identity Event.
    3. Criminal defense for charges brought against you as a result of a Stolen Identity Event. However, we will only pay for this after it has been established by acquittal or dropping of charges because you were not in fact the perpetrator.

A Stolen Identity Event is the fraudulent use of your personal identification, social security number, or other method of identifying you, including the fraudulent use of your personal identity to establish credit accounts, secure loans, enter into contracts or commit crimes. A Stolen Identity Event does not include the theft or unauthorized or illegal use of your business name, d/b/a or any other method of identifying your business activity.

- We shall pay you for the following in the event of an Unauthorized Electronic Fund Transfer:

1. The principal amount, exclusive of interest, incurred by you and caused by an Unauthorized Electronic Fund Transfer first occurring during the policy period. However, such principal amount shall not include any amount for which you did not seek reimbursement from the financial institution which issued the access device and holds the account from which funds were stolen, and for which you have not received reimbursement from any other source.
   An Unauthorized Electronic Fund Transfer (UEFT) is an electronic fund transfer from your Account initiated by a person other than you without the actual authority to initiate such transfer and from which you receive no benefit. An Unauthorized Electronic Fund Transfer (UEFT) does not include an electronic fund transfer initiated: 1) by a person who was furnished the access device to your account by you, unless you have notified the financial institution that transfers by such person are no longer authorized; 2) with fraudulent intent by you or any person acting in concert with you; 3) by the financial institution of its employee; or 4) from any business or commercial account.
   Account means a cash, credit card, demand deposit (checking), savings or money market account of yours held directly or indirectly by a financial institution and established primarily for personal, family or household purposes.

COVERAGE SCOPE

Subject to the Master Policy's terms, conditions and exclusions, the Master Policy provides benefits to you only if: (1) you report a Stolen Identity Event or an Unauthorized Electronic Fund Transfer to the Master Policyholder at the contact number stated above as soon as you become aware of a Stolen Identity Event or a Unauthorized Electronic Fund Transfer, but in no event later than ninety (90) days after the Stolen Identity Event or Unauthorized Electronic Fund Transfer is discovered; and (2) you follow the instructions given to you by the Fraud Resolution Unit. These instructions will include notifying major credit bureaus, the Federal Trade Commission's Identity Theft Hotline and appropriate law enforcement authorities. You will also be provided with a claim form and instructed how to file for benefits under the policy if the Stolen Identity Event or Unauthorized Electronic Fund Transfer results in losses covered under the policy.
You will only be covered for a Stolen Identity Event if a Stolen Identity Event is first discovered while you are a member of the Master Policyholder's insured program and is reported to us within ninety (90) days of such discovery.
You will only be covered for an Unauthorized Electronic Fund Transfer if an Unauthorized Electronic Fund Transfer first occurs while you are a member of the Master Policyholder's insured program and is reported to us within ninety (90) days of such discovery.
You will not be covered if the Stolen Identity Event or Unauthorized Electronic Fund Transfer first occurs after termination of the master policy or termination of your membership in the Master Policyholder's program.

LIMITS OF INSURANCE

The most we shall pay you are the Limits of Insurance shown above. All Legal Costs shall be part of and subject to the Aggregate Limit of Insurance. LEGAL COSTS ARE PART OF, AND NOT IN ADDITION TO, THE LIMIT OF INSURANCE.
Each aggregate sublimit of liability in this policy is the maximum limit of the Insurer's liability for all loss under the policy that is subject to that aggregate sublimit of liability. All sublimits of liability shall be part of, and not in addition to, the Limit of Insurance.
The Lost Wages Limit of Insurance shown above is a sublimit of the Aggregate Limit of Insurance and is the most we shall pay you for lost wages.

OTHER INSURANCE

We shall be excess over any other insurance, including, without limitation, homeowner's or renter's insurance. If you have other insurance that applies to a loss under this policy, the other insurance shall pay first. This policy applies to the

amount of loss that is in excess of the Limit of Insurance of your other insurance and the total of all your deductibles and self-insured amounts under all such other insurance. In no event shall we pay more than our Limits of Insurance as shown above.

DUPLICATE COVERAGES

If you are enrolled in more than one Membership Program insured by us, or any of our affiliates, we will reimburse you under each membership program:
a) subject to the applicable deductibles and Limits of Insurance of each insured Membership Program
b) but in no event shall the total amount reimbursed to you under all Membership Programs exceed the actual amount of loss.

From: Larry[redacted] [mailto:[redacted]@msn.com]
Sent: Friday, November 02, 2012 8:46 AM
To: Tom Davis
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry[redacted]

Thanks for your reply Tom,

However, this doesn't help the taxpayers that are or will be effected by this irresponsible action by the State of South Carolina.

1) I don't trust the governor, by the way she has handled this. It should have been disclosed earlier instead of a Friday afternoon news dump. The governor said that leaving Social Security numbers unencrypted is a common industry practice due to the complicated nature of the encryption process. T**his is not true.**

2) The State is going to provide monitoring for 1 year, so I assume the tax payer will be have to pay after the one year, which in some cases of children having their SS#, etc. listed on their parent's tax returns could go on for 70+ years. at $19.95 a month each.

3) No one has explain what Credit Fraud Resolution for life is. Does it mean if my SS# is used fraudently by a thief, that the State will be responsible for the necessary action to correct this theft? How long will it take? I am sure you have heard the horror stories.

Larry[redacted]

From: TomDavis@scsenate.gov
To: [redacted]@msn.com
Date: Thu, 1 Nov 2012 12:07:24 -0400
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

Dear Larry,

Like you, I was shocked last Friday to learn that computer systems at the S.C. Department of Revenue had been breached on numerous occasions, and that 3.6 million Social Security numbers and nearly 400,000 credit and debit card numbers had been obtained by what the governor's office has called "an international hacker." And I was stunned again yesterday when the governor announced the data of more than 650,000 businesses was also part of the hack.

For the past several days, I have communicated with the offices of Gov. Nikki Haley, SLED Chief Mark Keel, State Department of Revenue Director Jim Etter and others to learn more about this security breach. Obviously, state government has failed the people of South Carolina, and I pledge to you that an exhaustive inquiry will be conducted, that those guilty of malfeasance will be identified, and that appropriate steps will be taken to ensure that such sensitive information provided by citizens to their government is better protected in the future.

Tough questions will be asked and answers demanded. Questions such as: Why wasn't the credit card data kept in an unencrypted format? Was the breach the result of human error or inadequate security procedures? Why was data kept in a way that was accessible to the internet? What is the security audit process and how often is it conducted? What was the reason for the delay in advising the public of the security breach?

At this point, though, it is more productive to focus on how taxpayers can protect themselves, and to answer the most frequently asked questions. The information listed below in Q&A format has been provided by the governor's office, by Experian (the credit-protection agency retained by the governor's office), or by state newspapers who have assigned their best investigative reporters to uncover the facts. (In that latter regard, particular thanks are owed to The Greenville News; much of what is listed below can be found on its website.)

The governor's office provides regular updates on this situation, as do newspapers and other news outlets, and I post that information on my Facebook page and website as it becomes available. I invite you to visit https://www.facebook.com/senatortomdavis and/or www.senatortomdavis.com for that additional information.

Q: What steps do I need to take to protect my identity?

A: The governor and SLED chief said they do not know exactly what information was stolen, but they are urging anyone who filed a South Carolina tax return since 1998 to sign up for Experian's ProtectMyID service by calling 1-866-578-5422 or visiting the web site at protectmyid.com/scdor and using the activation code SCDOR123. The governor has said that the state will provide those affected with one year of credit monitoring and identify-theft protection.

Q: Are young adults that previously filed in SC covered by the consumer protection service?

A: If a tax return was filed from 1998 until present and a person's social security number 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.

Q: Do South Carolina residents need to do anything other than sign up with Experian to be fully protected?

A: In addition to the Experian product, state officials urge 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.

Q: If a South Carolina resident called and got a user name and password before the SCDOR123 code was announced, are they protected?

A: Yes.

Q: Do people have to call or can they do sign up online without calling?

A: If people have the signup code, they can go directly online to enroll. People are not required to call first. There are still people unaware of the online registration option and the call serves as the best means to inform them of that option.

Q: What about other credit reporting agencies? Do people need to sign up with them, or is that purely redundant?

A: Experian's ProtectMyID Alert is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus.

Q: What's the process for enrolling minor children in ProtectMyID?

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

Q: What are the requirements for getting my child covered under Family Secure?

A: Individuals must sign up for ProtectMyID first. Once they are registered, notification and a registration code (different from the one used for ProtectMyID) will be sent to them, with directions what to do to register minors with Family Secure. Those who registered online will receive this notification via email. Those who registered over the phone will receive the notification in the mail. This process will take two to three weeks. If you do not have minors listed as dependents, you can ignore the notice if you receive it. As with ProtectMyID, the Family Secure registration process may be completed via the phone with a live representative or online. Parents register their children as part of Family Secure.

Q: What are the benefits of Family Secure?

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

Family Secure coverage is for one adult and any number of minors. (Five minors can be enrolled via the website. For more than five, the customer must call Customer Care). The adult coverage includes a $2 million product guarantee covering the whole family, Score Tracker and Fraud Resolution.

Minors receive monthly monitoring for existence of a minor's credit report, and if a credit report is found, then we monitor for any changes to that report.

Q: How do I enroll my children in the identity theft protection plan?

A: The governor said during Tuesday morning's update that once you are signed up with Experian you will be notified by the company about enrolling minors in your family who have been associated to your Social Security number. According to the governor, if you are eligible to receive a family plan, the notification will arrive via e-mail if you signed up for the service online or a mailed letter if you signed up by calling the toll-free line.

Q: What period of time will this protection cover?

A: The governor said that those who sign up will be covered retroactively and they have until the end of January to get enrolled. Under a deal negotiated with Experian, South Carolina citizens whose tax returns were hacked will be eligible for credit fraud resolution for life, according to officials.

Q: What if I don't own a computer or have Internet access? Can I still enroll in the identity protection program?

A: Yes. Call 1-866-578-5422 to get assistance with enrollment over the phone. The governor said Tuesday that wait times averaged 10 minutes and that it took about nine minutes to get signed up once you get through.

Q: Why do I have to sign myself up? Why doesn't the state automatically sign the 3.6 million individuals potentially affected by the cyber hacking incident up for identity protection services?

A: The governor said that the state is not legally permitted to sign individuals up for a service in which they may not desire to participate.

Q: How much is this costing the state?

A: The governor said Tuesday morning that the state and Experian have agreed to cap security costs to the state at $12 million.

Q: Has the cyber hacker been identified or apprehended?

A: The SLED chief said no arrests have been made. Law enforcement officials have declined to answer specific questions about the investigation, describing it as "sensitive" and "complex."

Q: What exactly was taken?

A: The governor and SLED chief have said 3.6 million social security numbers and 387,000 mostly encrypted credit and debit card numbers were exposed, and that the data of more than 650,000 businesses was also part of the hack. Officials said they don't yet know how many of the numbers were actually taken, but said the scope of the breach includes anyone who has filed a South Carolina tax return since 1998.

Q: When did it happen?

A: The breach, the result of four intrusions into Revenue Department computers that began August 27 and continued until September 13, was discovered October 10. A Secret Service agent said the agency's computer crimes office first uncovered the intrusion and notified state authorities. The attack was not disclosed to the public until last Friday (September 26).

Q: Why wasn't the stolen information encrypted?

A: The governor said that leaving Social Security numbers unencrypted is a common industry practice due to the complicated nature of the encryption process. Some in the credit-security industry say encryption technology is readily available for data stores and is not cumbersome. Regardless, going forward, such data in South Carolina will be encrypted.

Q: Are other state agencies vulnerable to cyber hacking? Does other personal information remain at risk?

A: The governor asserted in a press conference that any agency, state or federal, can be hacked.

Tom Davis
Senator, Beaufort County
Senate District 46

Columbia Office:
P.O. Box 142
602 Gressette Building
Columbia, SC 29202
Tel: 202-212-6008 - Fax: 803-212-6299
Senate EMAIL: tomdavis@scsenate.gov

Beaufort Ofice:
Post Office Drawer 1107
1001 Craven Street
Beaufort, SC 29901-1107
Tel: 843-252-8583- Fax: 843-524-6401
District EMAIL: tom@senatortomdavis.com

From: Larry [redacted] [mailto:[redacted]@msn.com]
Sent: Thursday, November 01, 2012 9:38 AM
To: Tom Davis
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry [redacted]

This thing just keeps getting better!!!

Now we are told business information was stolen and they get treatment than individuals.

Like other S.C. taxpayers, state businesses will be able to get free credit monitoring. But companies will get longer coverage.
Businesses that have filed state taxes since 1998 can sign up for lifetime record monitoring from Experian starting today and Dun & Bradstreet starting Friday. Consumers can get one year of monitoring and insurance from Experian, paid for by the state. However, individual taxpayers will have to pay to continue the coverage after one year. Consumers will get lifetime credit-fraud resolution as part of Experian's agreement. The cost to the state for those services has been capped at $12 million.

Read more here: http://www.thestate.com/2012/11/01/2503354/657000-sc-business-records-also.html#storylink=cpy

I received a email back from the Director of Revenue CIO, thanks alot, basically giving me the same spin.

I asked her what lifetime credit-fraud resolution was and have heard nothing back.

Thanks

Larry [redacted]

From: TomDavis@scsenate.gov
To: [redacted]@msn.com
Date: Tue, 30 Oct 2012 14:38:38 -0400
Subject: RE: DOR SS# Info Hacked ~ Website email from Larry[redacted]

Senator Davis is currently reviewing the emails he has received from folks in his district concerning the security breach at SC DOR. In the meantime, I thought you may be interested in reviewing his comments in the recent Island Packet article. He has been monitoring and following this situation closely. Please let us know if you have any further information to share with our office.

Debbie Barthe
Office of Senator Tom Davis
Gressette Building 602
P.O. Box 142
Columbia, SC 29202
Phone: 803-212-6008
Fax: 803-212-6011
E-Mail: debbiebarthe@scsenate.gov

From: [redacted]@msn.com [mailto:[redacted]@msn.com]
Sent: Monday, October 29, 2012 9:54 AM
Subject: DOR SS# Info Hacked ~ Website email from Larry [redacted]

I am very upset about this! Why wasn't the Citizens informed when it happened in August? Why wasn't this information protected? What is being done to take care of this? SECURITY COMPROMISED SC officials plan on hacking update Monday morning Cyber-hacked SC taxpayers frustrated with help tips from state officials By CLIF LeBLANC - cleblanc@thestate.com E-MAIL PRINT REPRINT 57 COMMENTS TEXT SIZE: COLUMBIA, SC - Correction: The S.C. Consumer Affairs Department number is (800) 922-1594. As some South Carolina taxpayers, fearing their tax records have been hacked, complain about difficulties in getting access to the state's newly created self-help system, state leaders plan a Monday morning update on the massive security breach. Gov. Nikki Haley and SLED Chief Mark Keel have scheduled a 10.a.m. news conference at the State House. But an announcement from Haley%u2019s spokesman Rob Godfrey gives no indication of which aspects for the invasion of privacy case they plan to address. Video from around the world The governor%u2019s office also had scheduled a conference call at the same time for legislators. Godfrey said Sunday they will adjust the briefing to either just before or just after the news conference. Haley, Keel and other state and federal authorities on Friday disclosed that a foreign hacker or hackers had stolen 3.6 million Social Security numbers and 387,000 credit or debit card numbers from the S.C. Department of Revenue during a series of cyber attacks that date to Aug. 27. None of the data - except 16,000 of the credit card numbers %u2013 was encrypted, Revenue Department director James Etter said. State officials advised anyone who had filed a state tax return since 1998 to take steps to learn if their information had been misused by identity thieves. The state laid out procedures that worried taxpayers should take to determine if their information was misused and/or to protect themselves: Call (866) 578-5422, a hot line, to be given an access code to a website where they could register for one year of free credit monitoring. %u2022 A recording at the phone number provides a standard activation code (SCDOR123) that can be used at a web address: www.protectmyID.com/scdor. %u2022 The Revenue Department said it would have more receptionists at its call center over the weekend to help with the flood of calls. %u2022 The S.C. Consumer Affairs Department planned to add part-time staffers to answer phone calls during business hours starting today. Call (800) 922-1594 for advice or to request a freeze on your credit records. Privacy advocates say that is the surest way to block identity theft. Despite those steps, many South Carolinians were frustrated with the state%u2019s response over the weekend. Many emailed or called The State newspaper and other media outlets to vent, though some said they were given assistance through the hot line and the website. One woman complained she had trouble getting through to the web address that state officials provided. She decided to spend $35 to get a credit report to see if there was any unauthorized activity. A man said he got repeated recorded messages at the hot line and the web address was recited too quickly for him to write it down. He wrote the newspaper saying that his biggest worry remains: "whether or not I am one of whose records were stolen." Godfrey said Sunday that more people manned phone banks as soon as state officials learned of the phone delays. %u201CAnd the number of representatives has continued to increase over the weekend.%u201D By releasing the access code publicly, taxpayers should be able to speed the process of seeking credit protection, Godfrey said. %u201CIf we need to take any further action to make sure our taxpayers are protected, we will do so %u2013 and do so swiftly,%u201D the spokesman said. Read more here: http://www.thestate.com/2012/10/28/2499098/sc-officials-plan-on-hacking-monday.html#storylink=cpy

Larry [redacted]
[redacted]
Bluffton, SC 29909
843[redacted]

Pitts, Ted

From: Rep. Phyllis Henderson <[redacted]@gmail.com>
Sent: Sunday, November 04, 2012 11:06 PM
To: Pitts, Ted
Subject: Question about SSN

Ted:
If you read email below from my constitutent - what is the correct word about what SSN's were stolen. Does the State know or not know and when will you know, if not? Phyllis

---------- Forwarded message ----------
From: **Phyllis Henderson** <PhyllisHenderson@schouse.gov>
Date: Sun, Nov 4, 2012 at 11:03 PM
Subject: Fwd: Website email from Jerry [redacted]
To: Phyllis Henderson <[redacted]@gmail.com>

Rep. Phyllis Henderson
SC House District 21

Begin forwarded message:

> **From:** "[redacted]@bellsouth.net" <[redacted]@bellsouth.net>
> **Date:** November 4, 2012, 11:08:18 AM EST
> **Subject: Website email from Jerry [redacted]**
>
> I am seeing articles stating the DOR knows what SSN information has been hacked and other articles stating the DOR doesn't know. Can you clarify this for me? If they can determine SSN's that have been hacked, what is the means to find out? I also read that bank account information has also been hacked for those using direct deposit for refunds. Can you confirm this? Why is the state keeping bank information? I have been in the Information Technology field for 40 years. I have worked for multiple firms and have experienced that sensitive information is not only protected, it is also encrypted. Why this was not the practice of the DOR is an amazing example of incompetence.
>
> Jerry [redacted]
> [redacted]
> Greenville, SC 29615

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

Sign up for my DIstrict 21 newsletter! Click here:
http://oi.vresp.com?fid=58d852d7a6
On Twitter: @phyllish21
View my vote record: http://is.gd/henderson21 and click on "voting record"

Pitts, Ted

From: Bill Taylor <bill@taylorschouse.com>
Sent: Friday, November 02, 2012 1:46 PM
To: Pitts, Ted
Subject: Question EIN number

Another constituent question...
I promised her an answer.

-----Original Message-----
From: Kay [redacted] [mailto:[redacted]@yahoo.com]
Sent: Thursday, November 01, 2012 11:10 PM
To: bill@taylorschouse.com
Subject: SC Tax Issue regarding Hacking

Rep. Taylor,
I have gone to the website provided and added my SSN for the SC consumer protection, however it will not let me add my EIN number for my estate. I file a tax return on my estate each year and want to protect this also. So far no one can tell me what to do. Please help.
Thank you,
Kay [redacted]
803 [redacted]

Sent from my iPhone

Pitts, Ted

From: Adams, Marcia
Sent: Friday, November 02, 2012 11:57 AM
To: Joel Lourie
Cc: Pitts, Ted
Subject: RE: Possible Security Issue re job applicant ~ Website email from Mark [redacted]

Ms. Neal,
We are looking into this currently. We will help this customer and will be back in touch with you to provide additional information.

Thanks,
Marcia Adams

Marcia S. Adams
Executive Director | SC Budget & Control Board
1200 Senate Street | Columbia, SC 29201 | Office: (803) 734-2320

From: Joel Lourie [mailto:JoelLourie@scsenate.gov]
Sent: Friday, November 02, 2012 11:44 AM
To: Adams, Marcia; Pitts, Ted; Veldran, Katherine
Cc: '[redacted]@bellsouth.net'
Subject: FW: Possible Security Issue re job applicant ~ Website email from Mark[redacted]

Please see the email below from a concerned constituent who would like this security issue made aware to the state's human resource department and the Governor's office. Please do not hesitate to contact me if you have any information.

Take care,

Michele Neal
Senator Joel Lourie's office
P. O. Box 142
Suite 601 Gressette Building
Columbia, SC 29202
803-212-6116

From: [redacted]@bellsouth.net [mailto:[redacted]@bellsouth.net]
Sent: Friday, November 02, 2012 11:22 AM
Subject: Possible Security Issue re job applicant ~ Website email from Mark [redacted]

The State of SC , Dept. of Human Resources, has an on line system where people can fill out an application and submit those electronically for jobs. I used the system to apply for many state jobs. I decided I wanted to delete my account and application through SCDHR. I used the delete application button, and my application was deleted. After the SCDR incident, I was worried about my confidential data so I went back to the site. The application was not there. But -when I went to see jobs I had applied for (about 45 over the past 5 years) - every single one had a copy of my application so there (view application function) are basically 45 copies of my confidential application information floating around in a database not controlled by the State of SC. I contacted SCDHR and was told those applications COULD NOT be deleted, and that the data was totally secure. I was also told the State did not handle that, it was through a private company called "Governmentjobs.com" and "Neogov.com". I was told to call them to see if they could delete the 45 copies of my application. I called them, and discussed the issue with a customer service rep. They said there was no way to delete the info, but they would have someone contact me (no one did). I asked about the security and told them I was told the information was totally secure and the rep told me " no data can be toally secure, a hacker can always gain access if they know how" (I agree, that is true). So here are the issues: 1. I was never told and no where on the site did I see where it said the information I provided was going to a private company, and not the State of South Carolina. 2. The site does not warn anyone, that your infomation cannot be totally deleted once it is submitted. 3. It appears everyone who has ever used that site, no matter how long ago it was, has copies of their applications floating around in a data base (with internet access) for years and years. 4. If someone were to hack into the SCDHR application data, and combine it with the SCDR, they would have EVERYTHING needed to totally steal someone's identity including; where they went to school, every place they worked, where they work now, how much they make, etc. and all the usual highly confidential information on State applications. This is a serious issue, and needs to be addressed immediately. Everyone who has used the on line application for the State of South Carolina must be able to totally delete their accounts and all related data, for any reason. With the information being handled by a private company and not the State of SC, it is even more serious in my opinion. I deliberately did not apply to any on line job sites, because I did not want to provide my confidential information to some private company. Please see what can be done. I do not want another serious confidential data problem to pop up for our Governor, the state, or people in our state. This needs immediate attention. Thank you. Mark

Mark [redacted]
[redacted]
Columbia, SC 29206

Pitts, Ted

From: Rep. Phyllis Henderson <[redacted]@gmail.com>
Sent: Sunday, November 04, 2012 11:07 PM
To: Pitts, Ted
Subject: Question RE deceased persons

Ted:
Had a very good question/experience from a constituent below concerning her father, who died in 2010. Can you read this and explain to me what people are to do about covering a deceased person? Phyllis

---------- Forwarded message ----------
From: **Phyllis Henderson** <PhyllisHenderson@schouse.gov>
Date: Fri, Nov 2, 2012 at 7:59 PM
Subject: Fwd: SC security breach--deceased person ~ Website email from Paula[redacted]
To: Phyllis Henderson <[redacted]@gmail.com>

Sent from my iPhone

Begin forwarded message:

> **From:** "[redacted]@aol.com" <[redacted]@aol.com>
> **Date:** November 2, 2012, 4:15:33 PM EDT
> **Subject: SC security breach--deceased person ~ Website email from Paula [redacted]**
>
> Hi Phyllis, I am writing to ask that you clarify what action should be taken to help secure information that may have been stolen by the hackers for someone is has passed away. My father lived in SC for a few years until he passed away in October of 2010. He submitted tax returns under his social security number before his death, and we submitted tax returns under his new EIN number after his death. I called Experian and at first they told me that if anyone tried using his social security number, it would come up as a deceased person. Then I was told to send in his death certiicate along with several ofher pieces of information. Equifax also asked for several pieces of my private info as well to be sent by fax. Is my father's information safe without me going through all the additional steps with the 3 credit agencies? I am particularly uncomfortable sending my social security number and copy of my driver's license, etc. I would appreciate any information you may able to find that answers this question in a definitive manner. I must not be the only person in SC who has this type concern. Thank you in advance for your assistance Paula [redacted]
>
> Paula [redacted]
> [redacted]
> Greer, SC 29650
> 864-[redacted]

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

Sign up for my DIstrict 21 newsletter! Click here:
http://oi.vresp.com?fid=58d852d7a6
On Twitter: @phyllish21
View my vote record: http://is.gd/henderson21 and click on "voting record"

Pitts, Ted

From: Shwedo, Kevin A <Kevin.Shwedo@scdmv.net>
Sent: Monday, November 05, 2012 7:00 PM
To: Pitts, Ted
Cc: Valenta, Val; Murray, Larry G; McClary, Karl L; Devlin, Lotte; Phelps, Annie L; Sanderson, Jeffrey R; Woodhurst, Melinda S
Subject: RFI -- SCDMV support of State efforts to help mitigate data loss
Attachments: FAQ 11_2.pdf.pdf

Ted – per the Governors directive, SCDMV will support all initiatives to help mitigate data loss within the state. The following information is provided for your use and consideration:

- Below you will find a note from me to ALL DMV employees notifying them of the data breach and information as to how they can enroll in the Protect My Identity Program. The letter also mandates that all managers personally contact each employee and ensure each has had the time and opportunity to enroll themselves and each affected family member (NLT Friday, 9 November) in the program. I should be able to provide you 100% accountability by end of week.
- SCMDV will provide the State Inspector General a member of our Information Technology Staff for the next five weeks to assist in data collection, survey and investigation.
- SCDMV is prepared to assist citizens enroll in the Protect My Identify Program as required. Two options follow (in order of preference):
    - Option 1 -- SCDMV Customer Service Representatives would be trained and certified for one hour during our weekly mandatory training period (each Wednesday) and begin assisting citizens the following day. DMV would prepare forms for customers to fill out that would contain data to be entered by DMV employees and IMMEDIATELY returned to the person requiring assistance. No records would be created or maintained on our servers. There should be only minimal cost to the Department, but may slightly increase length of lines (last month we averaged 8 minutes per customer).
    - Option 2 -- SCDMV would require approximately $250,000.00 to purchase approximately 200 IPADs (with cellular service through the end of January) and support materials to provide "self service" enrollment capability. One Customer Service Representative would be available to answer technical computer questions, BUT WOULD NOT assist in data entry. The devices would be spread across DMVs based upon projected demand and shifted as demand changes.
- SCDMV can provide one page "fact sheets" to customers who would like more information on the breech and actions they can take to enroll in the Protect My Identity Program.

Please contact me immediately if there is anything else that would support the Governor's efforts to support DOR.

Thanks
Kevin

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!
"It's a GREAT day in South Carolina!"

From: Shwedo, Kevin A
Sent: Monday, November 05, 2012 6:21 PM
Subject: Employee Directive -- Protection Identity Protection provided for all those who filed SC taxes since 1998

Fellow Teammates – I think that each of you have heard that many South Carolina taxpayers and their children were victims of a data breach at the Department of Revenue. This is serious business and could adversely impact your credit rating IF someone steals your identity with the information gained. The State is going to give each of you the opportunity to obtain a free year of Credit and Identity Theft Protection from Experian (paid with state funds).

I want to make sure that EVERYONE at the DMV has been properly notified and given time to register themselves and their immediate family members. I am going to direct every manager to confirm whether you were given the opportunity and time to enroll. I am holding managers accountable for ensuring 100% accountability (just confirmation that you are aware of the service offered AND that you made a deliberate decision to either participate or deliberately delay your decision) before the end of business on Friday the 9th of November. If you choose to delay your decision you will still have until January 31, 2013 to enroll.

You can sign up by calling 1-866-578-5422 or by going to www.protectmyid.com/scdor and using the activation code "scdor123." 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.

I have personally enrolled all my affected family members via the published web site and found it to be relatively painless (there will likely be some wait time at the call center and virtually no wait time for the online service). The service is free. They DO NOT ask for your credit card information UNLESS you choose to sign up for additional, uncovered services. I chose to focus on the free services which I believe are adequate for me and my family.

I have attached some frequently asked questions that the State has received from constituents and legislators regarding the SC DOR security breach. I hope they answer some of the questions you may have – I will continue to send updates as I receive them. I do not have any more information available at this time, but wanted to provide you all the information I had access to. Thanks.

Kevin A. Shwedo
Executive Director
South Carolina Department of Motor Vehicles
Your SCDMV -- Each a Role Model; Competent, Committed, Courteous!

Pitts, Ted

From: Jim Etter <Etter_JF@sctax.org>
Sent: Tuesday, November 06, 2012 8:06 AM
To: Pitts, Ted; Stirling, Bryan
Subject: FW:
Attachments: Final Report Data Security DOR.docx

Thoughts????????

Jim Etter
Director
SC Department of Revenue
803-315-0192

From: Maley, Patrick [mailto:PatrickMaley@oig.sc.gov]
Sent: Tuesday, November 06, 2012 8:02 AM
To: Jim Etter
Cc: Davis, George
Subject:

Jim, attached are the electrons for the DOR policy compliance report dated October 9, 2012. Based on your call to the OIG shortly after receiving this report to hold the report in abeyance, but you were not at liberty to disclose the reason, was honored. With the public release of the hacker case, it became apparent that was the issue. The hacker incident did not change the DOR policy compliance review report, dated October 9, 2012. The report you originally got & still have, dated October 9, 2012, is our final report.

Of all of our compliance review reports, DOR was the only agency with no findings and likely no information that could identify vulnerabilities at DOR. However, due to the unique circumstances, I defer public release of the report to DOR. The OIG has no objections if DOR makes the determination to release the report. The other OIG policy compliance reports all potentially identify agency vulnerabilities and the OIG will not release at this time.

Thanks

Pitts, Ted

From: Martha Roof <Roof.Martha@doc.sc.gov>
Sent: Tuesday, November 06, 2012 11:34 AM
To: Pitts, Ted
Subject: Report for the Governor

Ted - Good morning – I am working on our report that is due COB today on how we are notifying and/or helping individuals to enroll in credit protection in light of the Cyber Attach at the SC department of Revenue based on the discussions at the cabinet meeting on last Thursday.

Do you want our report to be addressed **to you** *or to* **the Governor**?

Thanks

Martha Roof
SC Department of Corrections

Pitts, Ted

From: Ann Bowers <Bowers.Ann@doc.sc.gov>
Sent: Tuesday, November 06, 2012 3:46 PM
To: Pitts, Ted
Cc: Martha Roof
Subject: Letter to Governor Re: Security Breach at DOR
Attachments: DOC.PDF

Good afternoon Mr. Pitts,

Attached is a copy of a letter to Governor Haley explaining how the Department of Corrections keeping employees informed of updated information relative to the security breach at the Department of Revenue.

If you have any questions regarding the letter, please feel free to contact Ms. Martha Roof, Deputy Director for Administration, at 896-1744 or roof.martha@doc.sc.gov

I will be putting the original letter in the mail to you today.

Ann Bowers
S.C. Department of Corrections
Administration
803-896-1744

Pitts, Ted

From: Jim Etter <Etter_JF@sctax.org>
Sent: Tuesday, November 06, 2012 3:51 PM
To: Pitts, Ted
Subject: FW: Security Breach.pptx
Attachments: Security Breach.pptx

Ted,

This the DOR portion of the Library presentation on Friday.

They need a go no go tomorrow.

Thanks

Jim Etter
Director
SC Department of Revenue
803-315-0192

From: Sara Unrue
Sent: Tuesday, November 06, 2012 3:39 PM
To: Jim Etter
Cc: Nancy Wilson
Subject: FW: Security Breach.pptx

I've attached the current version of the PowerPoint presentation. I will be making a few revisions based on feedback received from the outreach team.

Thanks,
Sara Unrue

From: Sherry Blizzard
Sent: Tuesday, November 06, 2012 10:45 AM
To: Alvin "Mont" Alexander; Laura Watts (WattsL@sctax.org); John McCormack; Sherrie McTeer (MCTEERS@sctax.org); Nancy Wilson; Kimberly Haley; Samantha Cheek; Meredith Cleland (CLELANM@sctax.org); Milton Kimpson
Cc: Sherry Blizzard (BlizzaS@sctax.org); Sara Unrue
Subject: Security Breach.pptx

I am attaching a copy of the DOR presentation that would be used in the tentative webinar this Friday with the State Library, pending approval. This presentation could be used for other presentations, as well. I will bring copies to our 2:30 meeting. Please review and read the speakers notes at the bottom of the screen for any revisions needed. I did include copies of the screenshots that we received from Experian.

Pitts, Ted

From: Mike Shealy <MikeShealy@scsenate.gov>
Sent: Tuesday, November 20, 2012 3:50 PM
To: Pitts, Ted
Cc: Craig Parks; Lisa Catalanotto; Veldran, Katherine
Subject: Subcommittee Hearing

Ted,

As we discussed yesterday, the Finance Subcommittee to review the DOR information security breach will hold their first meeting on Wednesday, November 28th at 10:00 AM in Room 105 Gressette Building.

As part of the agenda, the subcommittee members would like for Marshall Heilman, the lead investigator for Mandiant, to come and testify. Should you feel that others involved in the investigation be available for clarification, please let me know. Since I don't have contact information for Mandiant, I would appreciate you informing the proper individuals about our request.

I would feel more comfortable if Chief Keel be in attendance at the meeting if for no other reason than to interject if questions or testimony approach the level of revealing information that might compromise any further investigation.

Additionally, the subcommittee would like for Mr. Etter or any other appropriate official at the Department of Revenue to testify. The goal in this segment is to establish technology security processes within the agency before the breach and learn of the improvements that have been implemented.

Finally, the subcommittee will call on Jimmy Early of the Division of State Information Technology at the Budget and Control Board to come and testify. The subcommittee wants to learn of the relationship between DSIT and the information technology staff at the Department of Revenue, focusing on the reasons why DOR chose not to use the security services of DSIT prior to the hacking incident.

As part of our preparation, we as staff will develop a list of questions for our members. And, we will share those questions with you so that the staff of DOR might be well prepared to answer questions directly and unambiguously.

Of course, if any of those testifying have handouts we are happy to make copies. Also, should anyone testifying desire to use a power point presentation, we have that capability too.

I anticipate at least two other meeting to be held. One will focus on the contractual arrangements made over the past several weeks. Another meeting will involve some expert testimony on best practices in cyber security.

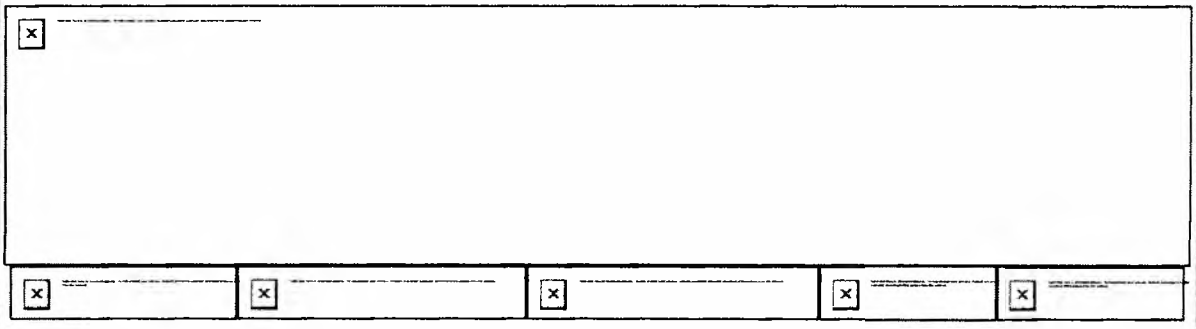
Thanks for your help.

Mike

Pitts, Ted

From: Rep. Bill Taylor <bill@taylorschouse.com>
Sent: Saturday, November 17, 2012 1:41 PM
To: Pitts, Ted
Subject: SENIOR ALERT - Identity Theft Protection - FAQs !

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



Senior Alert: Hacking FAQ's

(Informational Newsletter)

If you have not done so - please take steps to protect your identity.

Dear Friends:

South Carolina state government continues to roll-out specific and detailed information to assist the millions of residents whose personal information may be at risk due to the recent hacking of the computer system at the S.C. Department of Revenue. The Governor's office prepared the following answers to Frequently Asked Questions (FAQ's) aimed at S.C.'s senior citizens.

FOR SENIORS

Q: As a senior living in South Carolina, why should I be worried about identity theft?
A: The SC Department of Revenue announced on October 26, 2012 that taxpayers' records have been exposed in a cyber-attack. This includes Social Security numbers, credit and debit card numbers, and business tax filings.

Q: Who may have been affected by the security breach?
A: Individuals, their dependents and businesses who have filed a South Carolina tax return since 1998 to the present may have been affected.

Q: What should you do if you have filed a South Carolina tax return since 1998?
A: If you have filed a South Carolina tax return since 1998 to the present, the State is offering the opportunity to register with Experian's ProtectMyID™ protection plan free of charge for one year.

Q: What is Experian's ProtectMyID™ plan?
A: ProtectMyID™ is a service that monitors your credit and provides you alerts to any suspicious activity on your credit. ProtectMyID™ is designed to detect, protect and resolve potential identity theft, and includes daily monitoring of all three credit bureaus (Experian, Equifax, and TransUnion). 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.

Q: How do you sign up for the ProtectMyID™ service?

A: To sign up:

- *Call Experian's ProtectMyID™ Call Center at 1-866-578-5422 to register. You will talk to a live agent who will ask you certain questions in order to register you for the service. If you sign up for the service over the phone, you have the option for all future notices from Experian to be sent to you to your mailing address or to an email address, if you have one. Please note that each member of your household will need to call individually.*

OR

- *If you have access to the Internet and have an email address, you may go to www.protectmyid.com/scdor and use the activation code SCDOR123 to sign up. (Registering online is typically faster than registering by telephone.) If you register online, all future notices from Experian will be sent to your email address that you provide while registering. Experian is unable to send you notices to your mailing address if you sign up online.*

You do not need to sign up over the phone and online, but rather choose one option.

Q: What information do you need to register?
A: When registering, you will need to provide to Experian personal information such as:

- *Name*
- *Address*
- *Date of Birth*
- *Social Security Number*

As you are signing up for a free service, do not give out your credit card number when registering.

Q: How long will registering by telephone take?
A: There might be a wait time in order to speak with a representative. Please do not hang up while waiting as there will be a recorded message played before you are connected to a live representative.

The SC Department of Revenue or a credit bureau such as Experian will not initiate contact with you by phone, mail, or email to directly ask you for personal information such as your social security or credit card number.

Q: What are the hours of operation for the Experian® ProtectMyID™ Call Center?
A: Monday - Friday: 9:00 a.m. - 9:00 p.m. EST
Saturday and Sunday: 11:00 a.m. - 8:00 p.m. EST

Q: What benefits will a taxpayer receive after registering with ProtectMyID™?
A: Experian® will provide the following:

- *Credit Report: You will get a free copy of your Experian® credit report.*
- *Daily Credit Monitoring: You will receive alerts regarding any suspicious activity, including new*
- *inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian®,*
- *Equifax® and TransUnion® credit reports for one year.*
- *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.*
- *Identity Theft Insurance: If you have been a victim of identity theft, you will immediately be 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 for one year.

ExtendCARE: You will get full access to personalized assistance from a highly-trained Fraud Resolution Agent even after the initial one year ProtectMyID™ membership expires.

Q: Are there any other steps you can take to protect your identity?

A: There are other steps that you can take in order to further protect your identity:

1. *Regularly monitor your credit reports and review your bank statements.*
2. *Place fraud alerts with any one of the three credit bureaus (Experian, Equifax, TransUnion). When you alert one credit bureau, the other two will also be notified.*
3. *Place a freeze on your credit with each of the three credit bureaus; it is free to place a credit freeze. A credit freeze will prevent anyone accessing your credit without your permission. (Note: You will not be able to borrow money or obtain instant credit until you lift the freeze; after you contact the credit bureau to lift the freeze, you will be able to access your credit in about 30 minutes.)*

Q: Is there a deadline to register with ProtectMyID™?

A: January 31, 2013 is the deadline to register with ProtectMyID™.

Q: How much does it cost to register with ProtectMyID™?

A: ProtectMyID™ is free for South Carolina taxpayers for one year.

Q: What if I do not have a credit history with the credit bureaus?

A: If you do not have a credit history due to inactivity with your credit or otherwise, you will be able to register with a modified ProtectMyID™ plan.

Q: Can you explain (1) monitoring my credit reports and bank statements, (2) contacting a credit card and/or debit card issuer due to suspicious activity, (3) placing fraud alerts and/or credit freezes in more detail?

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

1. Review Your Credit Reports and Bank Statements.
We recommend that you remain attentive by reviewing your bank account statements and monitoring credit reports regularly. Under federal law, you are entitled once a year to one free copy of your credit report from each of the three major credit bureaus. You can also obtain a free credit report once a year by visiting www.annualcreditreport.com or calling 1-877-322-8228. You may wish to stagger your requests for each of these free credit reports so that you receive one 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 card or debit card information is compromised, the best protection is to obtain a new card with new card numbers. As stated above, it is recommended 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. You should tell your credit/debit card issuer that your account may have been compromised and should be reviewed for potentially fraudulent activity. If you use online banking, you may also want to change your credit/debit card account password immediately if you discover unauthorized charges.

3. Place fraud alerts and/or credit freezes. You can place a fraud alert with one of the three major credit bureaus (Experian, Equifax, TransUnion) by phone or by visiting their 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. Once you place

a fraud alert with one credit bureau, the other credit bureaus will also be notified. You also have the option of placing a credit freeze on your credit. You will need to contact all three of the credit bureaus in order to place a freeze and you will not be able to borrow money or obtain instant credit until you lift the freeze. If you need to lift the freeze at any time, you will need to contact the appropriate credit bureau to do so and your credit should be available in a matter of minutes. It is free to utilize the fraud alert and credit freeze options.

Credit Bureaus
If you need to contact the credit bureaus for reasons of placing a credit alert or credit freeze, please use the following contact information.

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

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

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

More Questions?
These FAQ's don't answer everything, so if you have a question send it to me. I'll do my best to get you an answer.

Please take this identity theft threat seriously.
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

Newsletter not paid for by
taxpayer funds.
Paid for by TaylorSCHouse


This email was sent to tedpitts@gov.sc.gov by bill@taylorschouse.com
Update Profile/Email Address | Instant removal with SafeUnsubscribe™ | Privacy Policy.
Bill Taylor for SC House District 86 | P.O. Box 2646 | Aiken SC | 29801