

Veldran, Katherine

From: Tommy Pope via Rally <team@rally.org>
Sent: Tuesday, October 30, 2012 2:44 PM
To: Veldran, Katherine
Subject: A new message from Tommy Pope

UPDATE FROM

Tommy Pope

via

RALLY



Share this



Post a comment



It was revealed last Friday that 3.6 million South Carolina Social Security numbers and 387,000 credit and debit card numbers were compromised in result of a cyber attack on a Department of Revenue server. Gov. Haley said this morning that the credit card numbers were from 2003 and have already expired, and that all security holes in state servers have since been "plugged."

Law enforcement is currently concentrating on bringing the hacker to justice. Gov. Haley said, the average time for seeing activity on a hacking is 6-8 months.

Anyone affected by the breach has until the end of January 2013 to call Experian and receive one year of free credit services. Minors listed as dependents on tax forms will be covered, as well.

Call 1-866-577-5422 or visit www.protectmyid.com/scdor and use the activation code "scdor123" to sign up. The protection covers all three credit agencies for one year, as well as fraud protection for life. Haley said 533,000 calls have come in and 287,000 people have signed up, since the call center opened. Although phone lines were clogged by news media constantly calling Friday, the current average wait time is 10 minutes.

View video of today's Statehouse press conference here:
http://www.youtube.com/watch?v=wleWyS8_VmA

[continue reading]

Give Now

Tommy Pope has 1116 supporters like you.



Manage email frequency or unsubscribe from further updates.

You can also get a weekly digest.

Fundraise for any cause

with Rally's free, social fundraising tools.

What do you rally for?

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



Veldran, Katherine

From: Stirling, Bryan
Sent: Sunday, October 28, 2012 3:22 PM
To: Veldran, Katherine; Pitts, Ted; Godfrey, Rob
Cc: Schimsa, Rebecca
Subject: Re: Fwd: Website email from Lisa Hoffman

Thank you, I have called him back and walked him through the process.

From: Veldran, Katherine
Sent: Sunday, October 28, 2012 02:43 PM
To: Stirling, Bryan; Pitts, Ted; Godfrey, Rob
Cc: Schimsa, Rebecca
Subject: Fw: Fwd: Website email from Lisa Hoffman

From: Garry R. Smith [<mailto:GarrySmith@schouse.gov>]
Sent: Saturday, October 27, 2012 07:13 PM
To: Veldran, Katherine
Subject: Fwd: Website email from Lisa Hoffman

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

Thanks!

Sent from my iPad

Begin forwarded message:

From: "[REDACTED]@aol.com" <[REDACTED]@aol.com>
Date: October 27, 2012, 4:52:56 PM EDT
Subject: Website email from Lisa Hoffman

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

Lisa Hoffman
204 Hunters Woods Dr
simpsonville, SC 29680

Veldran, Katherine

From: Schimsa, Rebecca
Sent: Sunday, October 28, 2012 9:14 AM
To: Stirling, Bryan
Cc: Pitts, Ted; Veldran, Katherine
Subject: Fw: From the Governor's Office re. cyber-attack at DOR

From: James Smith [mailto:JamesSmith@schouse.gov]
Sent: Sunday, October 28, 2012 05:59 AM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine; Mark Keel <mkeel@sled.sc.gov>; Kirkland T. Smith <Kirkland@KirklandSmith.com>; Rep. James E. Smith Jr. <James@JamesSmith.com>
Subject: Re: From the Governor's Office re. cyber-attack at DOR

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

Thanks, James

On Oct 26, 2012, at 4:46 PM, "Schimsa, Rebecca" <RebeccaSchimsa@gov.sc.gov> wrote:

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

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

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

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

Hacker illegally obtained credit card and Social Security numbers

COLUMBIA, S.C. – The South Carolina Department of Revenue today announced that approximately 3.6

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

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

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

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

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

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

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

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

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

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

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

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

-###-

VIDEO OF TODAY’S PRESS CONFERENCE:

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

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

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

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

1. Call 1-866-578-5422 where you will enroll in a consumer protection service. **The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit <http://www.protectmyid.com/scdor>. For the US Mail service, you will receive notifications via the US mail.

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

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

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

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

Directions:

1. Upon dialing the conference number, each participant will be asked his or her name and then be placed into the conference call.
2. Participants should plan to join the call 5-10 minutes prior to the start of the call.

3. Once the speakers have completed their statements, the call operator will provide instructions for the question and answer portion of the call.
4. All participants will be given the opportunity to ask questions.
5. Questions will be announced in the order that they are received.
6. For operator assistance at any time during the call, please press *0.

-###-

<Media Release from DOR 10.26.2012.pdf>

Veldran, Katherine

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

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

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

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

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

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

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

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

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

Representative Leon Stavrinakis
Stavrinakis Law Firm
843-813-2800

leon@stavlaw.net
leonstav@schouse.gov

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

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

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

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

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

Hacker illegally obtained credit card and Social Security numbers

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

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

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

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

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

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

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

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

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

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

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

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

-###-

VIDEO OF TODAY'S PRESS CONFERENCE:

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

in a cyber attack.

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

Video of the press conference is available here:

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

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

1. Call 1-866-578-5422 where you will enroll in a consumer protection service. **The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit <http://www.protectmyid.com/scdor>. For the US Mail service, you will receive notifications via the US mail.

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

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

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

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

Directions:

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

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

-###-

<Media Release from DOR 10.26.2012.pdf>

Veldran, Katherine

From: Larry Martin <lmartin@alicemfgco.com>
Sent: Friday, October 26, 2012 7:39 PM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine
Subject: Re: From the Governor's Office re. cyber-attack at DOR

Rebecca:

They did so. Unfortunately, one has to call the toll free number, and it's swamped. If everyone has to make the call as a precursor for signing up, it will take a long time to get everyone signed up.

Our Tigers did well last night! It was good to see a Thursday night game go so well.

Hope you have a great weekend.

Larry

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

From: Schimsa, Rebecca
To: 'lmartin@alicemfgco.com'
Cc: Pitts, Ted ; Veldran, Katherine
Sent: Friday, October 26, 2012 7:16 PM
Subject: Re: From the Governor's Office re. cyber-attack at DOR

Thank you for letting us know, Senator. I understand that our Chief of Staff, Bryan Stirling, has reached out to you in addition to our press office to walk you through the steps.

Please let us know if you have any further questions.

From: Larry Martin [mailto:lmartin@alicemfgco.com]
Sent: Friday, October 26, 2012 07:04 PM
To: Schimsa, Rebecca
Cc: Pitts, Ted; Veldran, Katherine
Subject: Re: From the Governor's Office re. cyber-attack at DOR

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

Thanks!

Larry

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

From: Schimsa, Rebecca
Cc: Pitts, Ted ; Veldran, Katherine
Sent: Friday, October 26, 2012 4:44 PM
Subject: From the Governor's Office re. cyber-attack at DOR

NEW INFORMATION INCLUDED.

Dear Members of the General Assembly,

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

Sincerely,

Rebecca Schimsa
Office of the Governor

MEDIA RELEASE FROM THE GOVERNOR'S OFFICE:

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

Hacker illegally obtained credit card and Social Security numbers

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

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

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

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

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

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

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

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

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

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

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

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

-###-

VIDEO OF TODAY'S PRESS CONFERENCE:

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

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

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

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

1. Call 1-866-578-5422 where you will enroll in a consumer protection service. **The call center is open 9:00 AM – 9:00 PM EST on Monday through Friday and 11:00 AM – 8:00 PM EST on Saturday and Sunday.**
2. Then you will determine if you wish to have an online or US Mail alert mechanism.
3. For the online service, visit <http://www.protectmyid.com/scdor>. For the US Mail service, you will receive notifications via the US mail.

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

-###-

CONFERENCE CALL INFORMATION FOR LEGISLATORS:

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

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

Directions:

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

-###-