Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Saturday, October 27, 2012 4:21 PM
To: Stirling, Bryan; Greg Young
Subject: Your message

Bryan:

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

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

Greg should be able to send you his comments soon.

Thanks

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

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

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

Stirling, Bryan

From: Jim Etter <Etter_JF@sctax.org>
Sent: Saturday, October 27, 2012 3:34 PM
To: Stirling, Bryan
Subject: Data file issue

The issue related to 5 records

Sent from my iPhone

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Saturday, October 27, 2012 3:31 PM
To: Stirling, Bryan
Cc: Brownd@sctax.org; Jim Etter (etter_jf@sctax.org)
Subject: Data file issue has been addressed

File will be uploaded by 1:30 PM pacific.

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

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

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

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Saturday, October 27, 2012 12:50 PM
To: Stirling, Bryan
Subject: I will call you at 1:30 Eastern

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

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

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

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

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Saturday, October 27, 2012 12:39 PM
To: Stirling, Bryan
Subject: Data file has formatting issues

Bryan:

We have been trying to load the file today but keep running into issues because the data is not formatted uniformly.

For example, some records list the last 4 of your SSN as 1 digit, others have zip codes with as many as 15 digits, and other records have multiple data points merged into single cells instead of multiple cells.

Is there any way that we can get a cleaner list for easier upload?

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

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

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

Stirling, Bryan

From: Ken Bixler <Ken.Bixler@experianinteractive.com>
Sent: Saturday, October 27, 2012 10:28 AM
To: Stirling, Bryan
Cc: Ozzie Fonseca; Michael Bruemmer; Ken Chaplin; Greg Young
Subject: Re: SCDOR status call

Bryan,
I'm asking Ozzie to follow up with you on status of the new recording. He has had some back and forth with outside counsel that it appears you may not have been copied on.

Thanks
Ken

Sent from my iPhone

On Oct 27, 2012, at 5:55 AM, "Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

I also believe we asked for the times to be EST and not PST.

From: Ken Bixler [mailto:Ken.Bixler@experianinteractive.com]
Sent: Friday, October 26, 2012 11:21 PM
To: Ozzie Fonseca <ofonseca@experianinteractive.com<mailto:ofonseca@experianinteractive.com>>; Michael Bruemmer <Michael.Bruemmer@experianinteractive.com<mailto:Michael.Bruemmer@experianinteractive.com>>; Ken Chaplin <Ken.Chaplin@experianinteractive.com<mailto:Ken.Chaplin@experianinteractive.com>>; Greg Young <Greg.Young@experianinteractive.com<mailto:Greg.Young@experianinteractive.com>>; Jim Etter (etter_jf@sctax.org<mailto:etter_jf@sctax.org>) <etter_jf@sctax.org<mailto:etter_jf@sctax.org>>; Stirling, Bryan; thad.westbrook@nelsonmullins.com<mailto:thad.westbrook@nelsonmullins.com> <thad.westbrook@nelsonmullins.com<mailto:thad.westbrook@nelsonmullins.com>>
Cc: Justin Greely <Justin.Greely@experianinteractive.com<mailto:Justin.Greely@experianinteractive.com>>
Subject: RE: SCDOR status call

Thad, Bryan and all –
As per our discussion earlier this evening, this is the process we are contemplating for the update call center flow. This relates to the provision of a "General Activation Code" that can be used for online enrollment purposes. All consumers calling the designated customer care number shall immediately hear a message that will read as follows:

Welcome to Experian Data Breach Resolution. If you are calling because you are a South Carolina resident and believe you have been impacted by the data breach recently announced, please listen carefully to this message in its entirety and write down the following:

Go to protectmyid.com/scdor<http://protectmyid.com/scdor> to use the following activation code to enroll in ProtectMyID Alert: SCDOR123.

Please be advised, only South Carolina residents are permitted to use this code. If the State of South Carolina has determined that you are not eligible, you will be given the opportunity to continue your membership at your expense, or your membership will be terminated.
If you do not have access to the website, you are not a South Carolina resident, or if you would like to speak to a representative for further assistance, please stay on the line.

The message may be played more than once in a loop to allow consumers to write down the General Activation Code provided. The expectation is a percentage of consumers will opt to use the General Activation Code provided and will drop off the call and go to the website where they will enroll via the code. This will hopefully be beneficial to call volumes and hold times.

As discussed, if a consumer is a not a SC resident or otherwise not eligible to use the General Activation Code they will nevertheless be permitted to enroll in the PMID Alert product. Experian will at a subsequent time reconcile the total number of consumers who have used the General Activation Code with the list provided by the State to determine if certain consumers who used the General Activation Code were in fact ineligible. The State shall not be charged for the ineligible memberships, and the ineligible consumers will be alerted that they may either continue the memberships at their expense or their membership will be terminated.

The timeline planned as of now is to launch the re-programmed messaging for incoming calls as of October 27th at 8 a.m. PT (11 a.m. ET). We will have a re-group discussion at 6 a.m. PT (9 a.m. ET) on Sunday October 28th to discuss the use of the General Activation Code and next steps.
Please respond to this e-mail with an acknowledgement that this is acceptable plan, or in the alternative let us know if there are any questions, concerns or points needing modification. Please note the recorded message length is subject to technical recording time constraints.

Thanks and best regards
Ken Bixler
Contracts Counsel
Experian Consumer Direct
949.567.7658

-----Original Appointment-----
From: Ozzie Fonseca
Sent: Friday, October 26, 2012 7:51 PM
To: Michael Bruemmer; Ken Bixler; Ken Chaplin; Greg Young; Jim Etter (etter_jf@sctax.org<mailto:etter_jf@sctax.org>); bryanstirling@gov.sc.gov<mailto:bryanstirling@gov.sc.gov>; thad.westbrook@nelsonmullins.com<mailto:thad.westbrook@nelsonmullins.com>
Subject: SCDOR status call
When: Sunday, October 28, 2012 6:00 AM-6:30 AM (UTC-08:00) Pacific Time (US & Canada).
Where: (855)-500-0023, Participant code 367567

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Friday, October 26, 2012 10:48 PM
To: Stirling, Bryan
Cc: Godfrey, Rob
Subject: RE: Experian PR contact

Rob -

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

Greg

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

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

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

-----Original Message-----
From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, October 26, 2012 7:38 PM

To: Stirling, Bryan
Subject: Re: Experian PR contact

Bryan,

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

GY

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

Sent by my iPhone

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

That works for me. Thank you.

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

Bryan:

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

Thanks

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

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

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

CONFIDENTIALITY NOTICE: This email message and any accompanying data or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the email address above, delete this email from your computer, and destroy any copies in any form immediately. Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other applicable privilege.

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

Thank you.

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

Bryan:

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

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

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

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

CONFIDENTIALITY NOTICE:
This email message and any accompanying data or files is confidential and may contain privileged information intended only for the named recipient(s). If you are not the intended recipient(s), you are hereby notified that the dissemination, distribution, and or copying of this message is strictly prohibited. If you receive this message in error, or are not the named recipient(s), please notify the sender at the email address above, delete this email from your computer, and destroy any copies in any form immediately. Receipt by anyone other than the named recipient(s) is not a waiver of any attorney-client, work product, or other applicable privilege.

-----Original Message-----
From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Friday, October 26, 2012 3:23 PM

To: Ozzie Fonseca
Cc: Greg Young; Thad Westbrook
Subject: RE: Experian PR contact

Thank you, call him now.

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

Bryan:

Here is our PR contact:

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

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

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

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

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Sunday, October 28, 2012 10:01 AM
To: Stirling, Bryan; Godfrey, Rob
Subject: From Greg Young, re: Post and Courier article

Gentlemen,

The article itself was not nearly as sharp-ended as the reporter, but I wanted to get your input on her last question. I feel it is bad for both of us to leave it unanswered, but I obviously did not want to jump in and say that it is definitely a risk and folks should continue to monitor, possibly implying the State is giving residents the short end of the stick.

If you are open to it, I'd like to craft messaging that addresses this question in a more holistic manner, reflecting the need to maintain vigilance all the time and providing other methods to monitor, in addition to the credit monitoring. It may benefit the messaging to also identify the difference between credit card fraud and identity theft, of which there seems to be confusion in the media, as well.

This would obviously be part of the FAQ document, but I think it may be something we want to provide separately, prior to the FAQ.

Thoughts?

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Sunday, October 28, 2012 10:41 AM
To: Milton Kimposon (kimpsonm@sctax.org); Thad Westbrook; Rush Smith; etter_jf@sctax.org; Stirling, Bryan
Cc: Michael Bruemmer
Subject: Family Secure memberships (minors)
Attachments: FamilySecure.pdf

All -

Thank you for your time this morning. As requested, I am providing you with pricing and product information regarding Family Secure (the product for minors).

Please note that each activation code allows a parent or guardian to enroll all children in the same household. In other words you will not have to pay a separate fee for each minor.

1 YEAR MEMBERSHIP (Fee Per Membership Activation)	
NUMBER OF MINORS AFFECTED	FAMILY SECURE (Experian Bureau)
50,000 - 100,000	$25.85
100,001 - 300,000	$21.95

I have attached a product sheet for your reference and also summarized the membership features below:

FAMILY SECURE

Parent or Legal Guardian:

- Daily monitoring of your Experian credit report with email notification of key changes
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Monthly "no-hit" reports: Updates letting you know there were no changes
- $2,000,000 product Guarantee
- Access to our toll-free customer care center
- Fraud resolution assistance: Toll-free access to fraud resolution representatives who investigate each incident; contact credit grantors to dispute charges, close accounts and compile documents; and contact all relevant government agencies

Children:

- Monthly monitoring to determine whether minors in your household have an Experian credit report
- Monthly monitoring alerts of key changes to your children's Experian credit report
- $2,000,000 product Guarantee
- Access to our toll-free customer care center
- Fraud resolution assistance: Toll-free access to fraud resolution representatives who investigate each incident; contact credit grantors to dispute charges, close accounts and compile documents; and contact all relevant government agencies

The website for enrollment is www.familysecure.com/enroll

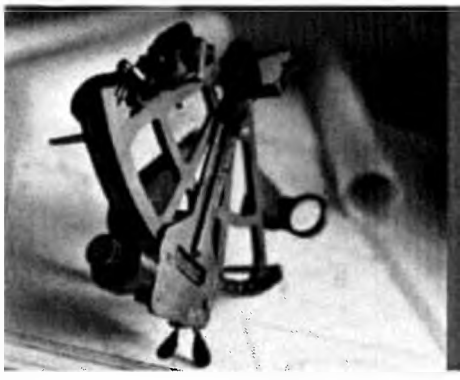
Please feel free to call me with any questions,

Regards,

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

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

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



Family Secure™

Online credit monitoring with a $2 Million Guarantee protects families against fraud and identity theft

Experian℠

Family Secure monitors credit report activity and provides email and text alerts of new changes, plus access to dedicated Fraud Resolution Agents.

Data breaches impact entire families – not just individuals

A data breach doesn't only affect your business, your staff and your customers. It impacts entire families when sensitive information of both adults and minors is exposed. The Federal Trade Commission counts as many as nine million victims of identity theft every year. That figure includes up to 500,000 children[1] some of who deal with the financial consequences for years.

The need for powerful identity protection following a data breach has never been greater. A data breach raises the risk of identity theft for affected individuals and, in turn, your risk for customer loss. Experian helps you minimize both risks with Family Secure. As a leader in data breach resolution, we've managed thousands of data breaches in nearly every industry.

We have dedicated professionals who will manage your case and provide assistance throughout the resolution process. We help you resolve a data breach rapidly and discreetly while maintaining employee and customer loyalty through monitoring and protection products like Family Secure.

Giving families the security of robust protection

As part of our data breach resolution solutions, Experian's Family Secure is ideal for data breaches impacting families. One parent can easily enroll online and then add all of their children at no additional cost.

Family Secure offers peace of mind through daily monitoring and support

- Daily monitoring of primary adult's credit report for 50 leading indicators of identity theft, such as new accounts, inquiries, addresses and more.
- Early warning alerts via email or mobile text message within 24 hours of detected credit report changes
- Regular monitoring of Experian information for every child on the account. Some minors have credit files if parents include them as co-signers on an account. If no credit file exists, Experian monitors for the creation of one in order to alert parents to new credit activity in a child's name.
- Comprehensive fraud resolution assistance helps members recover from identity theft quickly and efficiently. Each member has toll-free access to a dedicated Fraud Resolution Agent who investigates instances of identity theft, contacts creditors to dispute charges, close accounts and compile documents, and contacts relevant government and law enforcement agencies.
- Unlimited, on-demand access to Experian credit reports and credit scores 24/7.
- Monthly All Clear Alerts if no credit activity is detected in a month.
- Experian credit score illustrator to show monthly score trending and analysis.

$2 Million Family Secure Guarantee

- Up to $2 million maximum coverage with no deductible for active Family Secure members.[2]

Contact Ozzie Fonseca for more information at **Ozzie.Fonseca@Experian.com** or **1 949 567 3851**

Stirling, Bryan

From: Michael Bruemmer <Michael.Bruemmer@experianinteractive.com>
Sent: Sunday, October 28, 2012 4:15 PM
To: Stirling, Bryan
Cc: Greg Young; Ozzie Fonseca; Elizabeth Saucedo
Subject: Toll Number

Per your request

479-573-7373

Michael Bruemmer
VP, Data Breach Resolution
Experian
Phone-(949) 294-8886
www.experian.com/DataBreach

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Sunday, October 28, 2012 2:14 PM
To: Stirling, Bryan; Jim Etter (etter_jf@sctax.org)
Subject: Family Secure

Gentlemen:

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

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

Thanks

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

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

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

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Sunday, October 28, 2012 1:10 PM
To: Stirling, Bryan; Godfrey, Rob
Subject: FW: SC tax record hack

Gentlemen,

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

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

GY

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

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

Hey Greg,

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

Hope this makes sense.

Thanks,

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

Stirling, Bryan

From: Jim Etter <Etter_JF@sctax.org>
Sent: Sunday, October 28, 2012 9:14 PM
To: Stirling, Bryan; Pitts, Ted
Subject: Fwd: revised
Attachments: Schedule of project cost 1028.xlsx; ATT00001.htm

Sorry for the delay, staff has worked all to get best estimate

Jim

Sent from my iPhone

Begin forwarded message:

> **From:** "jim etter" <jimfetter@gmail.com>
> **Date:** October 28, 2012, 9:11:32 PM EDT
> **To:** "jim Etter" <etter_jf@sctax.org>
> **Subject: revised**

SOUTH CAROLINA DEPARTMENT OF REVENUE

Projected Incident Costs, *as of October 28, 2012*

Based on Returns as Filed (Some may have changed subsequently - Raw Data Captured)

ASSUMPTIONS	
Total # of Taxpayers Compromised	3,945,153
Total # of Taxpayers Compromised without Dependents	2,855,132
Total # of Taxpayers Compromised with Dependents	1,087,664
$ Cost per Taxpayer without Dependents for Credit Monitoring Service	$ 15.35
$ Cost per Taxpayer with Dependents for Credit Monitoring Service	$ 21.95
$ Cost per Taxpayer for Calling the Experian Call Center	$ 0.20

QUANTITY				COST				
Taxpayers Compromised Who May Sign-up for Credit Monitoring Service		# of Taxpayers Projected to Sign-up for Credit Monitoring Service		$ Cost for Credit Monitoring Service for Taxpayers		$ Cost for Calling the Experian Call Center	$ Cost for Other Expenses as Shown in Table Below	Total Cost
%	#	Without Dependents	With Dependents	Without Dependents	With Dependents			
15%	591,773	428,270	163,150	$ 6,573,941	$ 3,581,134	$ 118,355	$ 1,591,000	$ 11,864,430
20%	789,031	571,026	217,533	$ 8,765,255	$ 4,774,845	$ 157,806	$ 1,591,000	$ 15,288,906
30%	1,183,546	856,540	326,299	$ 13,147,883	$ 7,162,267	$ 236,709	$ 1,591,000	$ 22,137,859
40%	1,578,061	1,142,053	435,066	$ 17,530,510	$ 9,549,690	$ 315,612	$ 1,591,000	$ 28,986,813
50%	1,972,577	1,427,566	543,832	$ 21,913,138	$ 11,937,112	$ 394,515	$ 1,591,000	$ 35,835,766
70%	2,761,607	1,998,592	761,365	$ 30,678,393	$ 16,711,957	$ 552,321	$ 1,591,000	$ 49,533,672
90%	3,550,638	2,569,619	978,898	$ 39,443,649	$ 21,486,802	$ 710,128	$ 1,591,000	$ 63,231,578

OTHER EXPENSES	
$ Total Cost per Letters Mailed to Out-of-State Taxpayers Compromised[1]	$ 741,000
External IT Forensic Experts (Mandiant)	$ 500,000
External Legal Counsel (Nelson Mullins)	$ 100,000
External PR Firm (Chernoff)	$ 150,000
Miscellaneous	$ 100,000
Total Other Expenses	**$ 1,591,000**

Note 1: As known to date, there are 1.3M out-of-state taxpayers and the cost per letter is estimated to be $0.57. There is no requirement to mail letters to in-state taxpayers coompromised.

Taxpayers with dependents	
Filing Joint	494,256
Filing as Single	17,717
Filing as Head of Household	496,474
Filing as a widower	1,521
Unknown Status	77,696
Total	1,087,664

Taxpayers without dependents	
Filing Joint Primary Account	542,956
Filing Joint Secondary	542,956
Filing Joint Separate Not covered under the family Plan	494,256
Filing Married Separately	74,243
Filing as Single	1,199,035
Filing as Head of Household	165
Filing as a widower	1,521
Total	2,855,132

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Tuesday, October 30, 2012 12:48 AM
To: Stirling, Bryan; Godfrey, Rob
Cc: Michael Bruemmer; Ozzie Fonseca
Subject: From Greg Young, re: numbers for Call Center and ExtendCare info

Gentlemen,

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

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

ExtendCARE

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

Experian Fraud Resolution Agents specialize in:

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

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services

535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

freecreditreport.com
freecreditscore.com
creditreport.com
protectmyid.com
safetyweb.com

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Monday, October 29, 2012 5:34 PM
To: Stirling, Bryan; Godfrey, Rob
Cc: Michael Bruemmer; Ozzie Fonseca
Subject: From Greg Young, re: URGENT

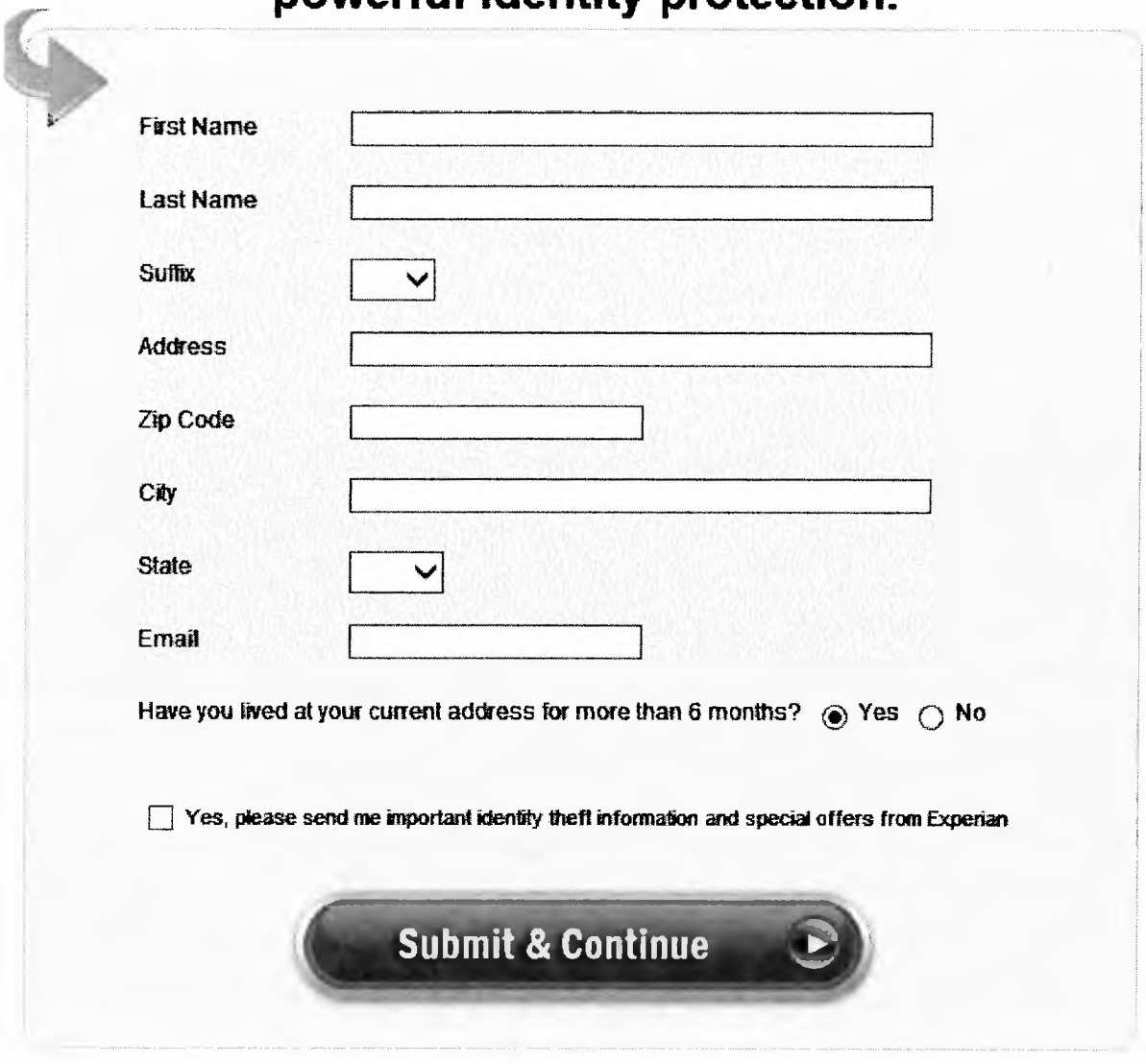
Gentlemen,

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

Best,

GY

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



Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

freecreditreport.com
freecreditscore.com
creditreport.com
protectmyid.com
safetyweb.com

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Monday, October 29, 2012 3:44 PM
To: Stirling, Bryan; Godfrey, Rob
Cc: Michael Bruemmer; Ozzie Fonseca
Subject: From Greg Young, re: FS overview

Gentlemen –

Here is a summation of FS:

Process:

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

Requirement:

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

Your other questions:

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

Family Secure features:

Coverage:

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

Key Benefits the adult receives:

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

Benefits the minors receive:

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

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

freecreditreport.com
freecreditscore.com
creditreport.com
protectmyid.com
safetyweb.com

Stirling, Bryan

From: Greg Foster <GregFoster@schouse.gov>
Sent: Wednesday, October 31, 2012 10:44 AM
To: Stirling, Bryan
Subject: Draft - Email & Webpost

Action Alert! - SC Taxpayers' Identities Hacked; Free Protection Available

Attention: This most likely affects you!

Anyone who has filed a South Carolina tax return since 1998 is potentially a victim of cyber identity theft. Free Protection is available to you, so please read this email carefully.

Last week, South Carolinians were notified of a serious cyber infiltration of sensitive private citizen information at our state's Department of Revenue. **Approximately 3.6 million Social Security Numbers and 387,000 credit card numbers were compromised in this cyber attack**.

To protect taxpayers, **the state is providing one year of FREE credit monitoring and identity theft protection by Experian ProtectMyID Alert**. While you have until January 31, 2013 to sign up, don't wait, it's important you act now to protect you identity from fraud and abuse. And again, **it's totally FREE**.

Hundreds of Thousands of South Carolinians have already signed up and are now protected.

While this cyber attack has raised a number of concerns that must be addressed, our immediate top priority is to make sure that every one of our state's 3.6 million citizens who have been affected get access to this free identity protection.

If you have filed a South Carolina tax return since 1998, here are the steps you need to take to access your free identity protection:

By Phone:

Call **1-866-578-5422** to enroll. The call center is open 9:00am to 9:00pm Monday-Friday & 11:00am to 8:00pm Saturday-Sunday. You can then determine if you would rather have an online or US Mail alert mechanism set up.

By Internet:

Sign up online at http://www.protectmyid.com/scdor. Enter the code **SCDOR123** when prompted. Then follow the quick and easy step-by-step instructions to enroll.

Again you have until January 31, 2013 to sign up...But please do it now, it's totally free.

Once you're enrolled, here are the protections that Experian will be providing you:

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, but you will continue to have access to fraud resolution agents and services beyond the first year. This complimentary 12-month

ProtectMyID memberships available to you includes:

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

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

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

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

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

Additionally, access to unlimited fraud resolution beyond the one year enrollment period is included in your Experian's ProtectMyID membership. You will also be notified – by email or letter – about how to sign up for a "Family Secure Plan" if you claim minors as dependents.

Please Act Now...

Now is not the time to point blame, but time to make sure all South Carolinians' identities are protected. There are several things that must be addressed following this cyber attack, many of which are already in motion, to better insulate sensitive data and help prevent future attempts to bypass our security measures. But right now, first and foremost, we must ensure that our citizens' identities are protected from fraud and abuse.

While there will no doubt be several exhaustive investigations into determining how exactly this cyber infiltration happened, what you can do right now is follow these steps to make sure your identity is protected.

Greg Foster
Deputy Chief of Staff
& Director of Communications
Office of the Speaker
South Carolina House of Representatives
(803) 734-3125
gregfoster@schouse.gov
twitter.com/gregfoster_sc

Stirling, Bryan

From: Dermody, Brandon <dermody@sostrategy.com>
Sent: Wednesday, October 31, 2012 10:52 AM
To: Stirling, Bryan
Subject: Invite
Attachments: Fraud Detection and Prevention in Government Programs Symposium.pdf

Here you go.

Thanks.

Fraud Detection and Prevention in Government Programs Symposium

Hosted by State Treasurer Curtis Loftis

Fraud and improper payments in government programs are on the rise nationally. Criminals have become increasingly more organized and sophisticated in their schemes to defraud limited government resources. It's a full-on assault against government programs by hidden attackers. In order to combat these threats, state government must become as sophisticated in our control as the criminals are in their schemes.

At this Fraud Detection and Prevention in Government Programs symposium, learn how modern technology can be used to detect sophisticated fraud schemes and organized criminal enterprises – before substantial losses are incurred. And learn best practices from both government and the private sector in the latest methods for detecting and preventing fraud, including:

- Current trends in fraud schemes and perpetrators
- Why an enterprise approach to fraud detection and prevention is critical to deterring today's fraud
- How advanced analytics, proven for years in the financial services industry, can help reduce government fraud
- How to incorporate continuous monitoring into the heart of government systems to prevent fraud and improper payments

WHAT: Fraud Detection and Prevention in Government Programs Symposium hosted by Treasurer Curtis Loftis

WHEN: November 13th from 8:30am until 11:30am

WHERE: Columbia Metropolitan Convention Center

Don't Get Burned

Speakers to include:

- *Curtis M Loftis, Jr.*: South Carolina State Treasurer
- *Patrick Maley*: South Carolina State Inspector General
- *Chris Swecker*: International expert on fraud and financial crimes; Former senior FBI executive and Chief Security Officer at Bank of America
- *Greg Henderson*: Government Practice Lead, Fraud and Financial Crimes Global Practice, SAS Institute

Agenda at a Glance
8:30 a.m. -- Registration and Networking
9:00 a.m. -- Welcome and introductions
9:10 a.m. -- Roundtable discussions
10:30 a.m. -- Q&A
11:00 a.m. -- Event wrap-up

To register, please respond to this email with your name, agency and title.

Thank you and we look forward to seeing you at the symposium!

Stirling, Bryan

From: Jason.Sweatt@ey.com
Sent: Wednesday, October 31, 2012 1:48 PM
To: Stirling, Bryan
Subject: Employer Identification Number Considerations

Hello, Bryan:

As we discussed, I wanted share some of the points that we discussed regarding Employer Identification Numbers (EINs).

While business taxpayer EINs are not published and available in a resource such as a public directory, most businesses do not consider them to necessarily be "confidential." They are used in too many places to truly be kept as tightly confidential as an individual's Social Security Number. It is also more difficult to use an EIN in conjunction only with an address to open credit lines or apply for credit cards. Generally, for a business, much more information is needed than the identifying information on the business' tax return.

Some places that they are used include:

- On employees' Forms W-2.
- On Forms 1099 issued to most providers of service to the company over $600.
- For public companies, on publicly published findings and readily available from the SEC.
- On certain permits and licenses required to be posted in a public place.
- For Tax Exempt organizations and certain other organizations, the entity's tax forms are public record.
- The numbers are issued to banks in application processes.
- The numbers are many times issued to customers and vendors for various reasons.
- Many other places

If I had a business client who had tax information compromised, whether any additional action was required would depend on the facts and circumstances. I would advise them to consider:

- Was the information taken already available to the general public. If so, no real breach of confidential information has really occurred.
- In the client's line of business, can the thief really take any action? What are the possible actions?
- Did the information contain sensitive information such as bank account numbers or credit card numbers, and were those accounts still active.
- Did the information that was taken include sensitive data, such as officers' salaries or officers' SSNs?
- Was the information taken information that would allow the thief to access other data (such as passwords for tax payments, etc.)

Based on the fact pattern, we would decide if any exposure had been created. If the data obtained was simply the identifying information of the business and potentially some financial data (numbers on the return), then for most businesses, they may not like the fact that a breach occurred, but in many cases real additional exposure for the business may not be created by a 3rd party obtaining limited information, even including the EIN.

Does that help?

Best Regards, Jason Sweatt

Jason C. Sweatt | Tax Quality & Risk Management
Ernst & Young LLP
75 Beattie Place, Suite 800, Greenville, SC 29601, United States of America
Direct: 1 864 298 3517 | Mobile: 1.864 320 1810 | Jason.Sweatt@ey.com
Fax: 1 866 586 8638 | EY/Comm: 7175277
Website: www.ey.com
Thank you for considering the environmental impact of printing emails.

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Wednesday, October 31, 2012 1:24 PM
To: Stirling, Bryan
Cc: Jon Neiditz; Thad Westbrook; Rush Smith (rush.smith@nelsonmullins.com); Michael Bruemmer; Ozzie Fonseca
Subject: From Greg Young, re: current numbers

Bryan,

Apologize for delay:

Calls: 620,000
Registrations: 418,000

Greg Young, APR
Director
Public Relations/Consumer Engagement

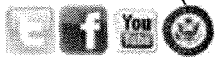
Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

freecreditreport.com
freecreditscore.com
creditreport.com
protectmyid.com
safetyweb.com

Stirling, Bryan

From: Perry, Richard (L. Graham) <Richard_Perry@lgraham.senate.gov>
Sent: Wednesday, October 31, 2012 1:52 PM
To: Stirling, Bryan
Subject: Letter to IRS re: EINs
Attachments: Shulman IRS.pdf

Richard S. Perry
Chief of Staff
Office of Senator Lindsey Graham
202-224-5972
202-224-3808 (fax)



LINDSEY O. GRAHAM
SOUTH CAROLINA

290 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5972

UNITED STATES SENATE

October 31, 2012

Commissioner Doug Shulman
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

Dear Commissioner Shulman,

I would like to bring to your attention an urgent matter related to Employer Identification Numbers or EINs. I was contacted by South Carolina Governor Nikki Haley about the prospect that several thousand private and public EINs were stolen from the S.C. Department of Revenue data banks.

I understand there is currently no system in place at the IRS to handle not only this particular type of ID theft, but this volume. Although in many cases EINs are readily available to the public through a myriad of sources including SEC filings, legitimate online search services, court filings, etc; I am asking you to prepare a protocol tailored specifically for South Carolina businesses that may want their EIN changed. Additionally, I'd ask that this service be made available to impacted businesses through your website and phone representatives.

I appreciate the responsiveness Catherine Barre and your entire agency have already provided me, the Governor's office and the S.C. Department of Revenue regarding the EIN issue. If you have any questions or I may be of assistance to the agency during this critical time for South Carolina's business community, please do not hesitate to contact me any time.

Sincerely,

Lindsey O. Graham
United States Senator

508 HAMPTON STREET
SUITE 202
COLUMBIA, SC 29201
(803) 933-0112

401 WEST EVANS STREET
SUITE 111
FLORENCE, SC 29501
(843) 669-1505

130 SOUTH MAIN STREET
SUITE 700
GREENVILLE, SC 29601
(864) 250-1417

530 JOHNNIE DODDS BOULEVARD
SUITE 202
MOUNT PLEASANT, SC 29464
(843) 849-3887

235 EAST MAIN STREET
SUITE 100
ROCK HILL, SC 29730
(803) 366-2828

124 EXCHANGE STREET
SUITE A
PENDLETON, SC 29670
(864) 646-4090

Stirling, Bryan

From: Perry, Richard (L. Graham) <Richard_Perry@lgraham.senate.gov>
Sent: Wednesday, October 31, 2012 2:21 PM
To: Stirling, Bryan
Subject: Need to send you a revised letter--Do NOT Distribute previous

Importance: High

There is a fact error—sending revised now-let me know if it was distributed

Richard S. Perry
Chief of Staff
Office of Senator Lindsey Graham
202-224-5972
202-224-3808 (fax)

Stirling, Bryan

From: Jason.Sweatt@ey.com
Sent: Wednesday, October 31, 2012 1:55 PM
To: Stirling, Bryan
Subject: RE: Employer Identification Number Considerations

Glad to help!

Best Regards, Jason Sweatt

Jason C. Sweatt | Tax Quality & Risk Management
Ernst & Young LLP
75 Beattie Place, Suite 800, Greenville, SC 29601, United States of America
Direct: 1 864 298 3517 | Mobile: 1.864 320 1810 | Jason.Sweatt@ey.com
Fax: 1 866 586 8638 | EY/Comm: 7175277
Website: www.ey.com

From: "Stirling, Bryan" <BryanStirling@gov.sc.gov>
To: "Jason.Sweatt@ey.com" <Jason.Sweatt@ey.com>
Date: 10/31/2012 01:52 PM
Subject: RE: Employer Identification Number Considerations

Thank you very much.

From: Jason.Sweatt@ey.com [mailto:Jason.Sweatt@ey.com]
Sent: Wednesday, October 31, 2012 1:48 PM
To: Stirling, Bryan
Subject: Employer Identification Number Considerations

Hello, Bryan:

As we discussed, I wanted share some of the points that we discussed regarding Employer Identification Numbers (EINs).

While business taxpayer EINs are not published and available in a resource such as a public directory, most businesses do not consider them to necessarily be "confidential." They are used in too many places to truly be kept as tightly confidential as an individual's Social Security Number. It is also more difficult to use an EIN in conjunction only with an address to open credit lines or apply for credit cards. Generally, for a business, much more information is needed than the identifying information on the business' tax return.

Some places that they are used include:

- On employees' Forms W-2.
- On Forms 1099 issued to most providers of service to the company over $600.
- For public companies, on publicly published findings and readily available from the SEC.

- On certain permits and licenses required to be posted in a public place.
- For Tax Exempt organizations and certain other organizations, the entity's tax forms are public record.
- The numbers are issued to banks in application processes.
- The numbers are many times issued to customers and vendors for various reasons.
- Many other places

If I had a business client who had tax information compromised, whether any additional action was required would depend on the facts and circumstances. I would advise them to consider:

- Was the information taken already available to the general public. If so, no real breach of confidential information has really occurred.
- In the client's line of business, can the thief really take any action? What are the possible actions?
- Did the information contain sensitive information such as bank account numbers or credit card numbers, and were those accounts still active.
- Did the information that was taken include sensitive data, such as officers' salaries or officers' SSNs?
- Was the information taken information that would allow the thief to access other data (such as passwords for tax payments, etc.)

Based on the fact pattern, we would decide if any exposure had been created. If the data obtained was simply the identifying information of the business and potentially some financial data (numbers on the return), then for most businesses, they may not like the fact that a breach occurred, but in many cases real additional exposure for the business may not be created by a 3rd party obtaining limited information, even including the EIN.

Does that help?

Best Regards, Jason Sweatt

Jason C. Sweatt | Tax Quality & Risk Management
Ernst & Young LLP
75 Beattie Place, Suite 800, Greenville, SC 29601, United States of America
Direct: 1 864 298 3517 | Mobile: 1.864 320 1810 | Jason.Sweatt@ey.com
Fax: 1 866 586 8638 | EY/Comm: 7175277
Website: www.ey.com

to advertise or promote a commercial product or service. You may choose not to receive advertising and promotional messages from Ernst & Young LLP (except for Ernst & Young Online and the ey.com website, which track e-mail preferences through a separate process) at this e-mail address by forwarding this message to no-more-mail@ey.com. If you do so, the sender of this message will be notified promptly. Our principal postal address is 5 Times Square, New York, NY 10036. Thank you. Ernst & Young LLP

Any U.S. tax advice contained in the body of this e-mail was not intended or written to be used, and cannot be used, by the recipient for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code or applicable state or local tax law provisions.

Stirling, Bryan

From: Perry, Richard (L. Graham) <Richard_Perry@lgraham.senate.gov>
Sent: Wednesday, October 31, 2012 2:29 PM
To: Stirling, Bryan
Subject: Revised IRS Letter (EINs)
Attachments: Shulman IRS Revised.pdf

Richard S. Perry
Chief of Staff
Office of Senator Lindsey Graham
202-224-5972
202-224-3808 (fax)

LINDSEY O. GRAHAM
SOUTH CAROLINA

290 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5972

UNITED STATES SENATE

October 31, 2012

Commissioner Doug Shulman
Internal Revenue Service
1111 Constitution Avenue, NW
Washington, DC 20224

Dear Commissioner Shulman,

I would like to bring to your attention an urgent matter related to Employer Identification Numbers or EINs. I was contacted by South Carolina Governor Nikki Haley about the prospect that several thousand private and public EINs were stolen from the S.C. Department of Revenue data banks.

Although in many cases EINs are readily available to the public through a myriad of sources including SEC filings, legitimate online search services, court filings, etc; I am asking you to prepare a protocol tailored specifically for South Carolina businesses that may want their EIN changed. Additionally, I'd ask that this service be made available to impacted businesses through your website and phone representatives.

I appreciate the responsiveness Catherine Barre and your entire agency have already provided me, the Governor's office and the S.C. Department of Revenue regarding the EIN issue. If you have any questions or I may be of assistance to the agency during this critical time for South Carolina's business community, please do not hesitate to contact me any time.

Sincerely,

Lindsey O. Graham
United States Senator

508 HAMPTON STREET
SUITE 202
COLUMBIA, SC 29201
(803) 933-0112

401 WEST EVANS STREET
SUITE 111
FLORENCE, SC 29501
(843) 669-1505

130 SOUTH MAIN STREET
SUITE 700
GREENVILLE, SC 29601
(864) 250-1417

530 JOHNNIE DODDS BOULEVARD
SUITE 202
MOUNT PLEASANT, SC 29464
(843) 849-3887

235 EAST MAIN STREET
SUITE 100
ROCK HILL, SC 29730
(803) 366-2828

124 EXCHANGE STREET
SUITE A
PENDLETON, SC 29670
(864) 646-4090

Stirling, Bryan

From: Director <director@sctax.org>
Sent: Wednesday, October 31, 2012 3:23 PM
To: Stirling, Bryan
Cc: Harry Cooper; etter_jf@sctax.org
Subject: FW: Business Credit Monitor - Press Urgent

Importance: High

From: Director
Sent: Wednesday, October 31, 2012 3:22 PM
To: 'tedpitts@gov.sc.gov'
Cc: Harry Cooper; etter_jf@sctax.org
Subject: FW: Business Credit Monitor - Press Urgent
Importance: High

I took this call and asked him to put it in email form to Director@sctax.org address.

Jenny Renedo
Office of the Director
SC Department of Revenue

From: Aaron Stibel [mailto:astibel@dandb.com]
Sent: Wednesday, October 31, 2012 2:58 PM
To: Director
Subject: Business Credit Monitor - Press Urgent
Importance: High

Thanks for taking my call and reviewing this email.

As a background I was with RSI for 12 years and was one of the original architects of DiscoverTax. I figured I would reach out directly since I know the state fairly well.

I am the CTO at Dun & Bradstreet Credibility Corp now . Jennifer with WISTV contacted our CMO about what we were doing for SC businesses. I understand that the press release does not mention specifically FEIN being compromised, but optically, this is becoming part of the story. We are planning to launch a South Carolina web site that will offer any SC business free business credit monitoring products.

We owe the press a call back ***today***, but I wanted to reach out to DOR so we can either keep you informed or have you be a part of this release. We would like the DOR to have input into how we position our release that best reflects the department's efforts.

I would suggest we have a call ASAP.

Please see our product offer below:

Dun & Bradstreet Credibility Corp will give SC businesses a free CreditAlert product that will help them stay alerted to changes in their scores or ratings and other indicators of fraudulent activity that could be taking place on their

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

Thanks,
-Aaron

Aaron Stibel
SVP, Technology
astibel@dandb.com
(310) 919 - 2214

Dun & Bradstreet
CREDIBILITY CORP

Stirling, Bryan

From: Glaccum, David (L. Graham) <David_Glaccum@lgraham.senate.gov>
Sent: Wednesday, October 31, 2012 3:29 PM
To: 'joseph.hicken@osd.mil'
Cc: Stirling, Bryan
Subject: SC Cyber Attack DOD Letter
Attachments: 10-31-12 SC Cyber Attack DOD Letter.pdf

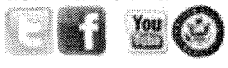
Joe,

Thanks for your help on this matter. The letter we sent to Under Secretary Wright is attached. We sent it out today.

The contact in South Carolina will be Bryan Stirling. His contact information is below. I have cc'd him on this message. Thank you again for your help in expediting this process. Please contact me if you have any questions. My direct dial is (202) 224-9413.

Bryan Stirling
Chief of Staff, Governor Nikki Haley
(803) 734-2100
bryanstirling@gov.sc.gov

David M. Glaccum
Deputy Counsel
Senator Lindsey O. Graham
290 Russell Senate Office Building
Washington, DC 20510
202-224-5972



LINDSEY O. GRAHAM
SOUTH CAROLINA

290 RUSSELL SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5972

UNITED STATES SENATE

October 31, 2012

Acting Principal Deputy Under Secretary of Defense for Personnel and Readiness
Jessica L. Wright
4000 Defense Pentagon
Washington, DC 20301-4000

Dear Under Secretary Wright:

On October 26, 2012, the South Carolina Department of Revenue released a statement regarding a cyber-attack involving the personal information of South Carolina taxpayers. Specifically, the attack exposed approximately 3.6 million Social Security numbers and 387,000 credit and debit card numbers. The security breach has the potential to impact a wide-range of South Carolinians, including a number who serve in our military. According to the South Carolina Division of Information Technology, the cyber attack occurred in mid-September, was discovered on October 16, and the system was closed and secured on October 20.

In response, the South Carolina Governor's Office has stated that the state of South Carolina will provide free credit monitoring and identity protection to South Carolina citizens that were affected by the cyber attack. To take part in this free service, citizens must contact a designated website or phone number and enroll. In addition to the monitoring service, state officials have provided additional steps citizens can follow to protect their identity.

The key to these services being effective is whether or not a citizen is informed of their availability. While their availability has been reported to citizens of South Carolina currently living in the state, it may not have reached our military personnel currently serving overseas. In an effort to ensure our men and women in uniform are made aware of the cyber attack and the free protective services, I am requesting that the United States Department of Defense contact the South Carolina Governor's Office and Department of Revenue, and coordinate a plan to contact our service members abroad. It is imperative that we inform all of those affected.

I am very concerned about this grave breach of privacy and am confident that, with your help, we will be able to protect our military personnel's personal information here at home.

I look forward to your timely response. Thank you.

Sincerely,

Lindsey O. Graham
United States Senator

508 HAMPTON STREET
SUITE 202
COLUMBIA, SC 29201
(803) 933-0112

401 WEST EVANS STREET
SUITE 111
FLORENCE, SC 29501
(843) 669-1505

130 SOUTH MAIN STREET
SUITE 700
GREENVILLE, SC 29601
(864) 250-1417

530 JOHNNIE DODDS BOULEVARD
SUITE 202
MOUNT PLEASANT, SC 29464
(843) 849-3887

235 EAST MAIN STREET
SUITE 100
ROCK HILL, SC 29730
(803) 366-2828

124 EXCHANGE STREET
SUITE A
PENDLETON, SC 29670
(864) 646-4090

Stirling, Bryan

From: Maley, Patrick
Sent: Wednesday, October 31, 2012 3:59 PM
To: Stirling, Bryan
Subject: FW: IG State-Wide Information Security Initiative--MEETING NOTIFICATION, 10AM, THURSDAY, 11/1
Attachments: Short Term Cyber Security Action Plan.docx; IT Agency Self Assessment.doc

---

From: Maley, Patrick
Sent: Wednesday, October 31, 2012 3:48 PM
To: 'Abdallah Haddad'; 'Alton "Al" Hoy'; Franklin, Ami; Ford, Andrew; 'Anthony Caldwell'; Bailey, Barbara; 'Barry Langley'; Hartman, Betsy; 'Bill Croteau'; 'Bill Hogue'; 'Bill Miller'; 'Bob Cape'; Boles, Les; Leach, Brian; Hoverman, Bryce; 'Camille Brown'; 'Candice Pou'; 'Catherine Lee'; Fallaw, Chuck; 'Cliff Stanley'; Smith, Dave; 'David "Ric" Lawson'; 'David Beverly'; 'David Elwart'; 'David Foshee'; Ross, David; Hipp, Dawn; 'Del Collins'; 'Don Cantrell'; 'Douglas Harper'; 'Elaine Knight'; Fletcher, Gayle; 'Guang Zhao'; Hammond, Carol; Harrill, Ken; 'Herbert Drucker'; 'James Hammond'; 'James Manning'; 'James Swindler'; MacDougall, James R.; 'Jay Rolin'; 'Jeff Baumann'; 'Jeffrey Smith'; 'Jim Bottom'; 'Jim Scurry'; 'Joan Assey'; 'John Dixon'; 'John Supra'; 'Katie Harrison'; Pondy, Kevin; Steele, Kevin; 'Khush Tata'; 'Larry Hubbard'; Nichols, Lisa; 'Margaret Sanders'; 'Mark Phipps'; Baker, Matt; 'Matt Faile'; 'Melissa Forinash'; Harris, Mike; 'Michael Wingard'; 'Michelle Moore'; 'Mike Garon'; 'Pam Everitt'; 'Pat Smith'; 'Paul Harmon'; Randy.Erskine; Dzek, Renee; 'Richard Nelson'; Rasmussen, Richard; Green, Richards; 'Robert Clark'; 'Robert Wilson'; 'Robin Lawrence'; 'Rolf Dolder'; 'Ron Mitchell'; 'Ronnie Finley'; 'Sandee Sprang'; Houston, Scott; Copeland, Sherry; 'Steve Flowers'; Sklar, Steve; 'Susan Worthy'; 'Thomas Smith'; 'Trad Robinson'; 'Trevis Shealy'; 'Troy Pound'; 'Yolanda McKnight'; 'jlowder@dew.sc.gov'; Adams, Marcia; Pitts, Ted; Earley, Jimmy; Jones, Sam; Oliver, Walt; 'bryanstirling@sc.gov.sc'
Subject: IG State-Wide Information Security Initiative--MEETING NOTIFICATION, 10AM, THURSDAY, 11/1

Attached to this email are the following **DRAFT** documents: 1) "short term cyber security action plan" for each agency; and 2) IT Agency Self-Assessment.

The 10AM, Thursday, 11/1 meeting is NOT MANDATORY for all CIOs; however, all CIOs/designee are encouraged & welcome. It is an opportunity to get direct and dynamic input on the attached **DRAFT** documents from those on the "front-line" of information security. Feel free to email me direct your input to be factored into the final documents. The meeting is also an opportunity to start the conversation and get input on developing a plan to fully assess state-wide information security.

I appreciate the talent and expertise in the agencies on information security. However, given the public's confidence level in state information security, we must double check ourselves as an initial step while we pursue a better understanding of this significant state-wide issue and opportunities to improve.

Thanks for your attention to this important issue.

10/30 IG email:

I was overwhelmed by the show of support for this effort--thanks. As set out in the below email last Friday & reinforced by media reports of the public's concern, we will be having a meeting at **10AM, Thursday, November 1, at the Forestry Commission, 5500 Broad River Road, Columbia**. The primary purpose of this meeting will be to seek input on immediate measures/protocols that can be deployed to agencies state-wide to

increase our collective information security confidence in the short-run, as well as identify critical weaknesses needing immediate attention.

To start the conversation, I will be sending an email out shortly (later today or Wednesday morning) containing a list of **DRAFT** recommendations from DSIT on this topic. Please look at this list prior to the meeting, and add/subtract/modify. We need everyone's experience & perspective on how best to swiftly check our own information security programs, deploy pragmatic measures, and identify any area that has immediate exposure to compromising PII.

Although the topic for this meeting will be a short-term response, similar to a military stand down day to re-emphasize and re-focus the importance of information security, the meeting will also start the process of planning a way forward to address longer-term issues.

I need four full-time volunteer subject matter experts from Agencies to fully staff the initial task force of six. I will personally lead this group. The group will set up the task force at DSIT offices, 4430 Broad River Road, Columbia. This task force will get it done in several months. We will add more staff if needed to hit that timeline rather than elongate a review given the significance and impact of the issue on the state. Please email me direct with your volunteer.

Thanks for your interest & support.

I
G Email to CIOs, Friday, 10/26:

If you have not already heard via media outlets, the Department of Revenue had a cyber intrusion resulting in the loss of 3.6 million names and social security numbers, as well as 387,000 credit card numbers. The Governor requested the Inspector General lead a state-wide information security (INFOSEC) initiative to assess our INFOSEC and make recommendations. This computer intrusion could have happened to anyone of us, but this large data loss of tax information has to impact our citizen's trust & confidence in state government to professionally protect their confidential information. After 30 years in the FBI, I don't get over-excited unless someone is shooting at me, but in my opinion, this is a crisis situation for information technology in state government.

I need your help. I am not an INFOSEC expert. My expertise is taking a mission, assembling the right team, developing objectives, collecting data on the objectives, and arriving at options & recommendations. I do know enough at this time to break this initiative into two phases. Phase I will identify measures or protocols to deploy to all agencies state-wide for immediate due diligence to give confidence to the public, as well as each other, that the collective IT components in state government are at a common quality assurance baseline. After our due diligence baseline, then Phase II will look at issues from a state-wide, longer term strategy perspective.

I will be assembling a team of subject matter IT experts to work full-time on this task force. I ask each agency CIO to think about voluntarily contributing a qualified staff member to this full-time task force. It will certainly be highly developmental, as well as contribute to an outcome having a long lasting impact on state government IT.

I am also soliciting volunteer CIOs to attend an initial organizing/strategy meeting to primarily address Phase I which has a time sensitive quality. If you are interested, please email me back at patrickmaley@oig.sc.gov or call my cell (803) 429-4946.

Due to time constraints, I am unable to send a copy to each of your respective Agency Heads for situational awareness, so I would appreciate you forwarding this email up your chain of command.

I will be back in touch to all CIOs early next week.

Thanks in advance for your time & interest in this critical initiative.

IG State-Wide Information Security Initiative
Short Term Cyber Security Action Plan

I. Short Term Remediation Steps

Immediately, all agencies should review and implement the following IT security measures:

1. All agencies should keep, monitor and review logs of all remote access, DNS, DHCP, Active Directory, and all systems in the DMZ. The logs should be stored for a minimum of 30 days or as required by statutes governing PII and other sensitive data.

2. Disable direct access to the Internet for all internal servers/data bases.

3. Ensure there are no data bases (no live data) in the DMZ.

4. Disable your local administrator account and have your administrators log in under their own named accounts. Some software requires local administrator access. In that case, the administrator password should differ from machine to machine.

5. Local accounts and domain accounts should have different user names and passwords.

6. Limit system accounts to a single purpose. Don't share system accounts across functions.

7. Disable dynamic DNS.

8. Ensure operating systems and 3rd party software are patched to the current level. Virus protection software must be maintained at its current level. These must be continuous processes.

9. Verify firewall egress and ingress rules to those ports required to do business.

10. Disable all credential caching on servers workstations laptops and mobile devices.

11. All servers in the DMZ should have only required services and network ports enabled.

II. Agency Self-Assessment

Self-assessments provide a cost-effective technique for agency officials to determine the current status of their information security programs, mitigate identified weaknesses, and where necessary, establish a target for improvement.

You must complete the information technology agency self-assessment survey linked below. Responses should be generated from multiple staff levels within the agency. Please note that you have to self-register prior to completing the survey.

Registration Instructions

Please have your staff complete each of the following surveys. New users will be required to validate their e-mail address prior to logging into the site. After your account has been activated by the website administrator an email will be sent to the email address you entered on the registration form with login instructions. You will need to identify a representative sample of staff from the categories below to complete the corresponding surveys.

Senior Management Survey
Operational Management Survey
IT Staff Survey
General Staff Survey

Assessment: https://sc-isac.sc.gov/content/information-technology-it-agency-self-assessment

III. Data Classification

Agencies will be asked to complete a data classification inventory. Instructions and templates will be provided in the next few days.

For Assistance

Please contact your DSIT Customer Service Representative if you need assistance with any of these measures.

Stirling, Bryan

From: Perry, Richard (L. Graham) <Richard_Perry@lgraham.senate.gov>
Sent: Wednesday, October 31, 2012 4:04 PM
To: Stirling, Bryan

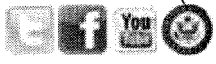
Bryan,

Below is additional info regarding EINs. There seems to be a lot of evidence that points to the fact that these numbers are public, or accessible fairly easily already. Some of this depends of the SC DOR protocol regarding the way they handle the privacy of such numbers; Below is additional info that may be helpful in fully understanding the seriousness or not of this particular breach.

For **public** companies, the EIN (or "IRS No.") is printed on the first page of 10-Ks, 20-Fs and other SEC filings, which you can get on the Internet for free (see the Filings section of "Securities and Exchange Commission").

For **private** companies, *it is possible* that the number is available on FreeErisa's EIN Finder or FEINsearch.com, or use the EIN field in the business search on a public records database such as KnowX.com, TLO, Accurint, Lexis (D&B;FEIN) or Westlaw (FEIN-ALL). If the company files with a Secretary of State the EIN may be on its annual report. If the company filed for bankruptcy, the EIN may be on the docket sheet as part the company's address. Also, EINs are often included in the company's D&B report (see "Dun & Bradstreet Reports").

Richard S. Perry
Chief of Staff
Office of Senator Lindsey Graham
202-224-5972
202-224-3808 (fax)



Stirling, Bryan

From: Harry Cooper <COOPERH@sctax.org>
Sent: Wednesday, October 31, 2012 4:20 PM
To: Stirling, Bryan
Cc: Pitts, Ted; etter_jf@sctax.org
Subject: FW: Returns/Vouchers Filed/Paid
Attachments: SoleProprietorship.pdf; Partnership.pdf; Corporation.pdf; LLC.pdf; Fiduciary.pdf

...more info on returns businesses file in sc and info on the returns.

From: Sherrie McTeer
Sent: Wednesday, October 31, 2012 4:17 PM
To: Harry Cooper
Cc: Mario Alvarez; Sherrie McTeer (MCTEERS@sctax.org)
Subject: Returns/Vouchers Filed/Paid

Harry,

Attached are separate files that include copies of returns by ownership type that a business may file. They are as follows: 1) Sole Proprietorship, 2) Partnership, 3) Corporation, 4) LLC and 5) Fiduciary.
After the cover sheet, there is a listing of typical forms a business may file. This is not all inclusive. Copies of the returns are also included.

For each return/payment voucher, we would key the primary number depending on the type tax. It may be social security number, SC file number or FEI. In addition we will key the period covered as listed on each return. All fields that have a delta ▶ beside the line item are also keyed and this data is captured and stored on our systems.

For the SC1040 (individual income tax return), all of the taxpayer's information - name, address, filing status, and dependent information is also keyed. These fields are not deltaed but are captured.

If you have any questions, please let me know.

Thanks...Sherrie

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Wednesday, October 31, 2012 4:58 PM
To: Stirling, Bryan
Subject: Your question

Bryan:

In response to your question, it is not necessary to buy additional credit reports to keep abreast of changes to your credit file. Upon enrollment the member will receive an Experian credit report as a baseline reference point, and from that point forward Experian provides monitoring of the 3 credit agencies for key changes to each respective credit file. If a change to any of those 3 credit files is detected, an alert will be sent to the member with enough details to help understand what has transpired, and enable the member to take further action as needed.

Since the alerts have specific details and are actionable it is not necessary to buy a new credit report to see the same information.

Regards,

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

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

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

Stirling, Bryan

From: Hicken, Joseph F CIV OSD LA <Joseph.Hicken@osd.mil>
Sent: Wednesday, October 31, 2012 5:08 PM
To: 'Glaccum, David (L. Graham)'
Cc: Stirling, Bryan
Subject: RE: SC Cyber Attack DOD Letter

Thanks David, per your request, I'll try to find someone Mr. Sterling can speak with before the letter is formally responded to.

v/r,
Joe

Joe Hicken
Office of the Assistant Secretary of Defense
for Legislative Affairs
Direct: 703.614.2865

-----Original Message-----
From: Glaccum, David (L. Graham) [mailto:David_Glaccum@lgraham.senate.gov]
Sent: Wednesday, October 31, 2012 3:29 PM
To: Hicken, Joseph F CIV OSD LA
Cc: bryanstirling@gov.sc.gov
Subject: SC Cyber Attack DOD Letter

Joe,

Thanks for your help on this matter. The letter we sent to Under Secretary Wright is attached. We sent it out today.

The contact in South Carolina will be Bryan Stirling. His contact information is below. I have cc'd him on this message. Thank you again for your help in expediting this process. Please contact me if you have any questions. My direct dial is (202) 224-9413.

Bryan Stirling

Chief of Staff, Governor Nikki Haley

(803) 734-2100

bryanstirling@gov.sc.gov

David M. Glaccum

Deputy Counsel

Senator Lindsey O. Graham

290 Russell Senate Office Building

Washington, DC 20510

202-224-5972

Description: S:\IT Stuff\GRAHAMicons_files\image002.jpg <http://twitter.com/GrahamBlog> Description: S:\IT Stuff\GRAHAMicons_files\image004.jpg <http://www.facebook.com/USSenatorLindseyGraham> Description: S:\IT Stuff\GRAHAMicons_files\image006.jpg <http://www.youtube.com/user/USSenLindseyGraham> Description: S:\IT Stuff\GRAHAMicons_files\image008.jpg <http://lgraham.senate.gov/public>

Stirling, Bryan

From: Jeff Stibel <jstibel@dandb.com>
Sent: Wednesday, October 31, 2012 4:08 PM
To: Stirling, Bryan
Cc: Judy Hackett; Aaron Stibel
Subject: Re: SC

Thanks Bryan - confirmed and approved.

On Oct 31, 2012, at 1:05 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> As we discussed we'd like this Credit Alert to be available to any business that has filed a tax return from 1998 to the breach date with SC. Please approve, thank you.

Stirling, Bryan

From: Jeff Stibel <jstibel@dandb.com>
Sent: Wednesday, October 31, 2012 6:16 PM
To: Stirling, Bryan
Cc: Judy Hackett; Aaron Stibel
Subject: Re: SC

No problem Bryan. To fully clarify, "for life"is a bit vague so we should be sure that it is life of the product (i.e., we could be out of business in 200 yrs and I can't imagine that product being live then in any event). I just want to make sure no one is seeming disingenuous. But in the spirit of our conversation, our goal is to help these businesses out long term until this problem is resolved.

Best,

Jeff

On Oct 31, 2012, at 3:09 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> Thank you for doing this for life.
> That's what we told the press.
>
> ---
>
> **From:** Judy Hackett [mailto:jhackett@dandb.com]
> **Sent:** Wednesday, October 31, 2012 6:02 PM
> **To:** Stirling, Bryan; Jeff Stibel; Aaron Stibel
> **Subject:** RE: SC
>
> We can certainly do this for the life of the product. Offering anything for life is an odd thing because we could be talking about 100 years. It might be better for you to come up with a reasonable amount of time. Let us know either way.
>
> Judy Hackett
> Chief Marketing Officer
> Dun & Bradstreet Credibility Corp
> 22761 Pacific Coast Highway
> Malibu, CA 90265
> O: 310-919-2233
> C: 770-337-4869
> F: 310-919-2948
> www.DandB.com
>
> <image001.png>

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Wednesday, October 31, 2012 2:54 PM
To: Judy Hackett; Jeff Stibel; Aaron Stibel
Subject: RE: SC

I recall someone saying on the phone with the governor that it was for life. Came someone please verify this? We told the press that.

From: Judy Hackett [mailto:jhackett@dandb.com]
Sent: Wednesday, October 31, 2012 5:52 PM
To: Stirling, Bryan; Jeff Stibel; Aaron Stibel
Subject: RE: SC

This is a product we typically charge monthly annually for. Our thinking was that the right amount of time was a year or so. Thoughts?

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

<image002.png>

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Wednesday, October 31, 2012 2:49 PM
To: Jeff Stibel; Aaron Stibel
Cc: Judy Hackett
Subject: Re: SC

If this a for life product? So if I was a SC business would I get this product for life?

From: Jeff Stibel [mailto:jstibel@dandb.com]
Sent: Wednesday, October 31, 2012 04:37 PM
To: Aaron Stibel <astibel@dandb.com>
Cc: Stirling, Bryan; Judy Hackett <jhackett@dandb.com>
Subject: Re: SC

Great. They are in the middle of the announcement now. Be sure to send them a note when the link is live with the URL as a reminder.

On Oct 31, 2012, at 1:35 PM, "Aaron Stibel" <astibel@dandb.com> wrote:

Team:

We will have a simple SC Coming Soon page up on DandB.com/SC in the next few moments.

We can change this page; I just didn't want the Governor's office to announce something without at least a Coming Soon page up.

This page will be replaced with the actual offer page tomorrow night.

-Aaron

Aaron Stibel
SVP, Technology
astibel@dandb.com
(310) 919 - 2214

<image001.jpg>

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Wednesday, October 31, 2012 1:08 PM
To: Jeff Stibel
Cc: Judy Hackett; Aaron Stibel
Subject: RE: SC

Thank you very much!

From: Jeff Stibel [mailto:jstibel@dandb.com]
Sent: Wednesday, October 31, 2012 4:08 PM
To: Stirling, Bryan
Cc: Judy Hackett; Aaron Stibel
Subject: Re: SC

Thanks Bryan - confirmed and approved.

On Oct 31, 2012, at 1:05 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

As we discussed we'd like this Credit Alert to be available to any business that has filed a tax return from 1998 to the breach date with SC. Please approve, thank you.

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Wednesday, October 31, 2012 5:45 PM
To: Stirling, Bryan
Cc: Jon Neiditz; Thad Westbrook; Rush Smith (rush.smith@nelsonmullins.com); Michael Bruemmer; Ozzie Fonseca; Ken Bixler
Subject: From Greg Young, re: numbers for 2:30 pm PST 10-31-12

Bryan –

Numbers:

Calls: 630,000
Registrations: 455,000
Avg. Wait time: 12 min.

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com

Stirling, Bryan

From: Routh, Billy <brouth@hsbcopperdome.com>
Sent: Thursday, November 01, 2012 3:47 PM
To: Stirling, Bryan
Cc: Godfrey, Rob; Erin Hardwick Pate
Subject: FW: News Alert - SC Businesses Offered Free Credit Monitoring

Please pass along to Governor Haley the SC Association of Certified Public Accountants (SCACPA) has provided information to their nearly 4000 members statewide in an effort to inform their membership and their clients of the security breach at SCDOR. SCACPA continues to work closely with the SCDOR to insure the most accurate and updated information is being provided.

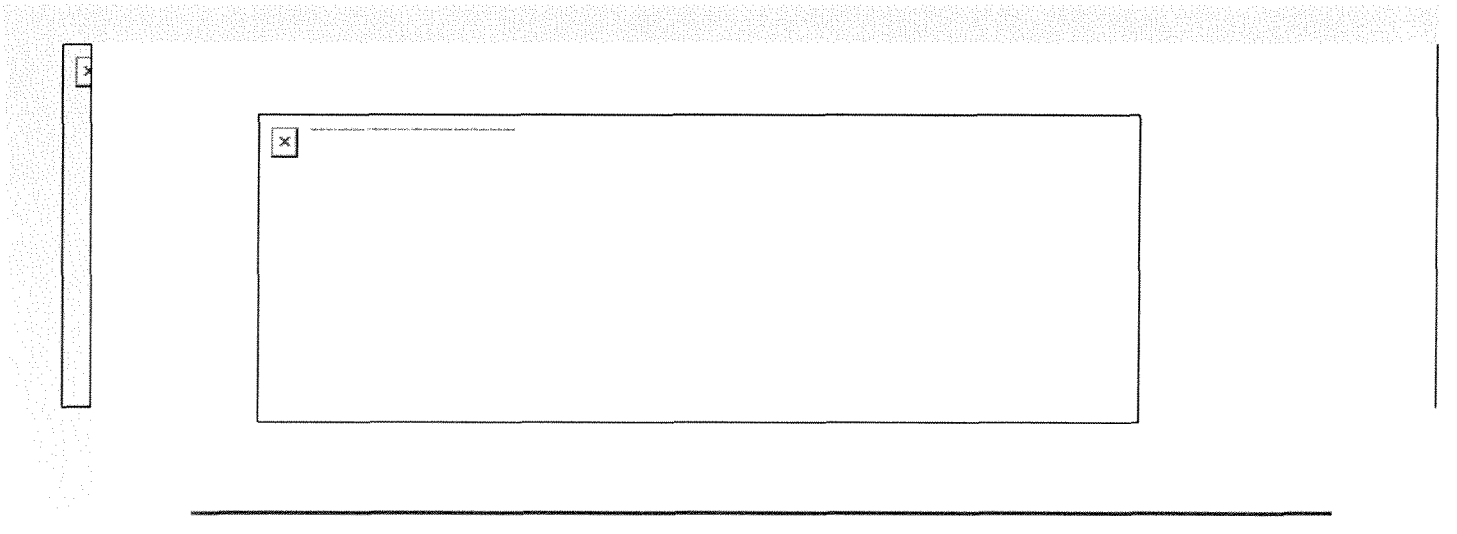
SCACPA stands ready and willing to assist further moving forward.

Please let me know if you have any questions.

From: Erin Hardwick Pate [mailto:ehardwickpate@scacpa.org]
Sent: Thursday, November 01, 2012 3:32 PM
To: Routh, Billy
Subject: News Alert - SC Businesses Offered Free Credit Monitoring

Begin forwarded message:

> **From:** "South Carolina Association of CPAs (SCACPA)" <acowherd@scacpa.org>
> **Date:** November 1, 2012, 2:49:41 PM EDT
> **To:** Erin Test, Erin H. <ehardwick@scacpa.org>
> **Subject: [MARKETING] News Alert - SC Businesses Offered Free Credit Monitoring**
> **Reply-To:** acowherd@scacpa.org



SCACPA is following the latest developments in the S.C. Department of Revenue security breach and will send updates as they become available. In addition, we encourage you to email your questions to mtaylor@scacpa.org. We are in contact with SCDOR, the governor's office, the IRS and other agencies and will post responses to the SCACPA website. Additional resources are also available on the SCACPA website.

Update: Protection for businesses available at no charge

It was announced Oct. 31 that information from up to 657,000 businesses was exposed in the security breach at SCDOR.

The state has arranged fraud monitoring for businesses from Dun & Bradstreet Credibility Corp. for S.C. businesses.

Beginning Nov. 2 at 8 a.m., South Carolina businesses that have filed a tax return since 1998 can sign up at http://www.dandb.com/sc/ or call customer service toll free at the dedicated phone number 1-800-279-9881. The CreditAlert product will alert customers to changes taking place in their business credit file.

Experian is offering impacted South Carolina businesses Business Credit AdvantageSM - a self-monitoring service that allows unlimited access to a company's business credit report and score. Beginning Nov. 1, South Carolina businesses can sign up for Business Credit AdvantageSM at http://www.smartbusinessreports.com/SouthCarolina.

View a video of the Oct. 31 Statehouse press conference here: http://www.youtube.com/watch?v=rYohFHnQaE8.

SCACPA | 570 Chris Drive | West Columbia | SC/29169 |

(803) 791.4181

Follow Us:

***IRS CIRCULAR 230 NOTICE**: Internal Revenue Service regulations generally provide that, for the purpose of avoiding federal tax penalties, a taxpayer may rely only on formal written advice meeting specific requirements. Any tax advice in this message, or in any attachment to this message, does not meet those requirements. Accordingly, any such tax advice was not intended or written to be used, and it cannot be used, for the purpose of avoiding federal tax penalties that may be imposed on you or for the purpose of promoting, marketing or recommending to another party any tax-related matters.*

Stirling, Bryan

From: SC Small Business Chamber of Commerce <sbchamber@scsbc.org>
Sent: Thursday, November 01, 2012 2:46 PM
To: Stirling, Bryan
Subject: Re: Problem with Experian

Great. I'll let her know.

From: Stirling, Bryan
Sent: Thursday, November 01, 2012 2:33 PM
To: mailto:sbchamber@scsbc.org
Subject: Re: Problem with Experian

Yes, any one who registers will get an email or letter, depending on how they registered, informing them how to register their minor children. Need to be a parent or legal guardian to register minors.

From: SC Small Business Chamber of Commerce [mailto:sbchamber@scsbc.org]
Sent: Thursday, November 01, 2012 02:16 PM
To: Stirling, Bryan
Subject: Problem with Experian

Bryan,
It was nice to talk to you yesterday during the press conference. I wanted to call your attention to something I just heard from one of my Board members who tried to register her daughter's name with Expirian. The dates of birth for registration only go back to 1994. Therefore all children in the state with SS#s, the prime targets of identity theft folks, are not protected.

Is there anyway for you to address this with Expirian?
Thanks,
Frank

Stirling, Bryan

From: Jack Pringle <jpringle@ellislawhorne.com>
Sent: Thursday, November 01, 2012 11:48 AM
To: Stirling, Bryan
Subject: CIPP-US Designation/Hawkins Lawsuit

Bryan- as we discussed on the phone, I have recently obtained designation as a Certified Information Privacy Professional (CIPP-US) through the International Association of Privacy Professionals. This designation involves knowledge and background in U.S. privacy law and regulations, and in particular data breaches and the evolving law surrounding same. My bio can be found at the link below:

https://www.linkedin.com/[redacted]

I have obtained a copy of the Hawkins lawsuit, and have had a chance to review same. I would welcome the opportunity to discuss same with you and/or other members of the Governor's staff. In addition, I also have experience in class action defense, and have been on the other side of Mr. Hawkins in the putative class action cases involving the payday lending industry.

Best,

Jack P.

John J. Pringle, Jr.
jpringle@ellislawhorne.com | 803.386.7452 google voice

ELLIS : LAWHORNE
Ellis, Lawhorne & Sims P.A., Attorneys At Law

1501 Main Street, 5th Floor, Columbia, South Carolina 29201
803.254.4190 tel | 803.779.4749 fax | www.ellislawhorne.com

SC Business Law Blog | My Bio | LinkedIn - Profile | Firm Web Site | My V-card

Stirling, Bryan

From: Glaccum, David (Judiciary-Rep) <David_Glaccum@judiciary-rep.senate.gov>
Sent: Thursday, November 01, 2012 7:51 PM
To: Stirling, Bryan
Subject: Fw: Timeline?

----- Original Message -----
From: Glaccum, David (L. Graham)
Sent: Thursday, November 01, 2012 05:54 PM
To: Glaccum, David (Judiciary-Rep)
Subject: FW: Timeline?

From: Hicken, Joseph F CIV OSD LA
Sent: Thursday, November 01, 2012 5:54:24 PM (UTC-05:00) Eastern Time (US & Canada)
To: Glaccum, David (L. Graham); Miller, Andrea LtCol OSD LA
Subject: RE: Timeline?

David, we're working it. Problem is that we don't have an automatic instrumentality to reach out to SC domiciled personnel who are deployed (in general), and let them know their information has been compromised by the state, from the OSD level. Trying to get folks to work out a creative solution.

v/r,
Joe

Joe Hicken
Office of the Assistant Secretary of Defense for Legislative Affairs
Direct: 703.614.2865

-----Original Message-----
From: Glaccum, David (L. Graham) [mailto:David_Glaccum@lgraham.senate.gov]
Sent: Thursday, November 01, 2012 5:12 PM
To: Hicken, Joseph F CIV OSD LA; Miller, Andrea LtCol OSD LA
Subject: Timeline?

Thank y'all again for the assistance in this matter. Would y'all be able to offer a timeline of when someone will be in contact with Bryan at the Governor's office? The sooner the better. He wants to start up a dialogue ASAP so they can begin to develop a plan. Thank you.

DMG

David M. Glaccum

Deputy Counsel

Senator Lindsey O. Graham

290 Russell Senate Office Building

Washington, DC 20510

202-224-5972

Description: S:\IT Stuff\GRAHAMicons_files\image002.jpg <http://twitter.com/GrahamBlog> Description: S:\IT Stuff\GRAHAMicons_files\image004.jpg <http://www.facebook.com/USSenatorLindseyGraham> Description: S:\IT Stuff\GRAHAMicons_files\image006.jpg <http://www.youtube.com/user/USSenLindseyGraham> Description: S:\IT Stuff\GRAHAMicons_files\image008.jpg <http://lgraham.senate.gov/public>

Stirling, Bryan

From: Neil Rashley <nrashley@scbankers.org>
Sent: Thursday, November 01, 2012 6:06 PM
To: Stirling, Bryan
Subject: Re: SCBA - DOR Database Breach

9am or anytime after 12.

Sent from my iPhone

On Nov 1, 2012, at 5:59 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> Sure. What time?
>
> ---
>
> **From:** Neil Rashley [mailto:nrashley@scbankers.org]
> **Sent:** Thursday, November 01, 2012 5:59 PM
> **To:** Stirling, Bryan
> **Subject:** Re: SCBA - DOR Database Breach
>
> Could we have a Monday meeting? Fred Green, our new CEO, is out of town until then. FYI he's the former CEO of NBSC and Synovus. Very knowledgeable banker.
>
> Neil
>
> Sent from my iPhone
>
> On Nov 1, 2012, at 4:22 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:
>
> > Thank you for your offer and taking time to talk today. I will keep you posted and reach out to you.
> >
> > ---
> >
> > **From:** Neil Rashley [mailto:nrashley@scbankers.org]
> > **Sent:** Thursday, November 01, 2012 4:20 PM
> > **To:** Stirling, Bryan
> > **Subject:** SCBA - DOR Database Breach
> >
> > Bryan,
> >
> > Thanks for calling me back. I know this is a constantly evolving situation but we wanted to make sure the Governor's Office used us as one of its primary sources of information for what banks do, especially in these situations. Also, we have been communicating with our bankers and trying to give them the most up-to-date information so they can advise their customers.
> >
> > So, here's our points:
> >
> > - Please use us as the primary source for the Governor's Office on what banks do and what they can offer.
> > - Keep us updated as to the extent of taxpayers' bank account information that has been accessed.

- If there is any way we can assist in helping you inform the public, then we will help.
- You mentioned a meeting and we would like to meet as soon as possible.

Thanks and contact me at any time.

Neil Rashley
Senior Vice President and Counsel
South Carolina Bankers Association
2009 Park Street
P.O. Box 1483
Columbia, SC 29202
(803) 779-0850
(803) 467-221 (cell)
(803) 256-8150 (fax)
nrashley@scbankers.org
www.scbankers.org

Stirling, Bryan

From: Neil Rashley <nrashley@scbankers.org>
Sent: Thursday, November 01, 2012 6:04 PM
To: Stirling, Bryan
Subject: Re: SCBA - DOR Database Breach

Checking with Fred.

Sent from my iPhone

On Nov 1, 2012, at 5:59 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> Sure. What time?
>
> ---
>
> **From:** Neil Rashley [mailto:nrashley@scbankers.org]
> **Sent:** Thursday, November 01, 2012 5:59 PM
> **To:** Stirling, Bryan
> **Subject:** Re: SCBA - DOR Database Breach
>
> Could we have a Monday meeting? Fred Green, our new CEO, is out of town until then. FYI he's the former CEO of NBSC and Synovus. Very knowledgeable banker.
>
> Neil
>
> Sent from my iPhone
>
> On Nov 1, 2012, at 4:22 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:
>
> > Thank you for your offer and taking time to talk today. I will keep you posted and reach out to you.
> >
> > ---
> >
> > **From:** Neil Rashley [mailto:nrashley@scbankers.org]
> > **Sent:** Thursday, November 01, 2012 4:20 PM
> > **To:** Stirling, Bryan
> > **Subject:** SCBA - DOR Database Breach
> >
> > Bryan,
> >
> > Thanks for calling me back. I know this is a constantly evolving situation but we wanted to make sure the Governor's Office used us as one of its primary sources of information for what banks do, especially in these situations. Also, we have been communicating with our bankers and trying to give them the most up-to-date information so they can advise their customers.
> >
> > So, here's our points:
> >
> > - Please use us as the primary source for the Governor's Office on what banks do and what they can offer.
> > - Keep us updated as to the extent of taxpayers' bank account information that has been accessed.

- If there is any way we can assist in helping you inform the public, then we will help.
- You mentioned a meeting and we would like to meet as soon as possible.

Thanks and contact me at any time.

Neil Rashley
Senior Vice President and Counsel
South Carolina Bankers Association
2009 Park Street
P.O. Box 1483
Columbia, SC 29202
(803) 779-0850
(803) 467-221 (cell)
(803) 256-8150 (fax)
nrashley@scbankers.org
www.scbankers.org

Stirling, Bryan

From: Glaccum, David (L. Graham) <David_Glaccum@lgraham.senate.gov>
Sent: Thursday, November 01, 2012 11:57 AM
To: Stirling, Bryan
Subject: RE: SC Cyber Attack DOD Letter

That is odd. We sent the letter to the Under Secretary on Personnel. Joe Hicken, the gentleman that emailed you yesterday, told me he was going to expedite the letter so that the Under Secretary would get it and contact you. Hopefully that will happen today. If it doesn't, feel free to contact Joe directly, but I assume they are trying to get you in contact with the highest authority available. I can also put another call in, if you don't hear something soon.

David M. Glaccum
Deputy Counsel
Office of Senator Lindsey Graham

-----Original Message-----
From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Thursday, November 01, 2012 11:46 AM
To: Glaccum, David (L. Graham)
Subject: RE: SC Cyber Attack DOD Letter

Still waiting on DOD contact to call me. Thank you.

-----Original Message-----
From: Glaccum, David (L. Graham) [mailto:David_Glaccum@lgraham.senate.gov]
Sent: Wednesday, October 31, 2012 5:10 PM
To: 'Hicken, Joseph F CIV OSD LA'
Cc: Stirling, Bryan
Subject: RE: SC Cyber Attack DOD Letter

Thank you. Please let me know if there is anything I can do to help.

DMG

David M. Glaccum
Deputy Counsel
Office of Senator Lindsey Graham

-----Original Message-----
From: Hicken, Joseph F CIV OSD LA [mailto:Joseph.Hicken@osd.mil]
Sent: Wednesday, October 31, 2012 5:08 PM
To: Glaccum, David (L. Graham)
Cc: bryanstirling@gov.sc.gov
Subject: RE: SC Cyber Attack DOD Letter

Thanks David, per your request, I'll try to find someone Mr. Sterling can speak with before the letter is formally responded to.

v/r,
Joe

Joe Hicken
Office of the Assistant Secretary of Defense for Legislative Affairs
Direct: 703.614.2865

-----Original Message-----
From: Glaccum, David (L. Graham) [mailto:David_Glaccum@lgraham.senate.gov]
Sent: Wednesday, October 31, 2012 3:29 PM
To: Hicken, Joseph F CIV OSD LA
Cc: bryanstirling@gov.sc.gov
Subject: SC Cyber Attack DOD Letter

Joe,

Thanks for your help on this matter. The letter we sent to Under Secretary Wright is attached. We sent it out today.

The contact in South Carolina will be Bryan Stirling. His contact information is below. I have cc'd him on this message. Thank you again for your help in expediting this process. Please contact me if you have any questions. My direct dial is (202) 224-9413.

Bryan Stirling

Chief of Staff, Governor Nikki Haley

(803) 734-2100

bryanstirling@gov.sc.gov

David M. Glaccum

Deputy Counsel

Senator Lindsey O. Graham

290 Russell Senate Office Building

Washington, DC 20510

202-224-5972

Description: S:\IT Stuff\GRAHAMicons_files\image002.jpg <http://twitter.com/GrahamBlog> Description: S:\IT Stuff\GRAHAMicons_files\image004.jpg <http://www.facebook.com/USSenatorLindseyGraham> Description: S:\IT Stuff\GRAHAMicons_files\image006.jpg <http://www.youtube.com/user/USSenLindseyGraham> Description: S:\IT Stuff\GRAHAMicons_files\image008.jpg <http://lgraham.senate.gov/public>

Stirling, Bryan

From: Neil Rashley <nrashley@scbankers.org>
Sent: Friday, November 02, 2012 10:18 AM
To: Stirling, Bryan
Subject: RE: SCBA - DOR Database Breach

Thanks for putting the meeting together. Who from your office will attend?

Right now I anticipate we will have me, Fred and another banker.

Don't worry. Our intentions are to have a professional, informational meeting and to offer what we can to assist.

Neil

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Thursday, November 01, 2012 6:00 PM
To: Neil Rashley
Subject: RE: SCBA - DOR Database Breach

Sure. What time?

From: Neil Rashley [mailto:nrashley@scbankers.org]
Sent: Thursday, November 01, 2012 5:59 PM
To: Stirling, Bryan
Subject: Re: SCBA - DOR Database Breach

Could we have a Monday meeting? Fred Green, our new CEO, is out of town until then. FYI he's the former CEO of NBSC and Synovus. Very knowledgeable banker.

Neil

Sent from my iPhone

On Nov 1, 2012, at 4:22 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> Thank you for your offer and taking time to talk today. I will keep you posted and reach out to you.
>
> ---
>
> **From:** Neil Rashley [mailto:nrashley@scbankers.org]
> **Sent:** Thursday, November 01, 2012 4:20 PM
> **To:** Stirling, Bryan
> **Subject:** SCBA - DOR Database Breach
>
> Bryan,
>
> Thanks for calling me back. I know this is a constantly evolving situation but we wanted to make sure the Governor's Office used us as one of its primary sources of information for what banks do, especially in these situations. Also, we have been communicating with our bankers and trying to give them the most up-to-date information so they can advise their customers.
>
> So, here's our points:

- Please use us as the primary source for the Governor's Office on what banks do and what they can offer.
- Keep us updated as to the extent of taxpayers' bank account information that has been accessed.
- If there is any way we can assist in helping you inform the public, then we will help.
- You mentioned a meeting and we would like to meet as soon as possible.

Thanks and contact me at any time.

Neil Rashley
Senior Vice President and Counsel
South Carolina Bankers Association
2009 Park Street
P.O. Box 1483
Columbia, SC 29202
(803) 779-0850
(803) 467-221 (cell)
(803) 256-8150 (fax)
nrashley@scbankers.org
www.scbankers.org

Stirling, Bryan

From: Ozzie Fonseca <ofonseca@experianinteractive.com>
Sent: Friday, November 02, 2012 1:01 AM
To: Stirling, Bryan
Subject: Requested numbers

Bryan:

Thank you for your note. I am not certain if I replied to you directly so i'm doing it now.

I forwarded your note to Greg so that he could arrange for the numbers to be sent to you as requested. I don't believe that web traffic statistics will be available since the landing page used for your engagement is shared. However, we're looking into separating your traffic going forward.

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

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

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

Stirling, Bryan

From: Neil Rashley <nrashley@scbankers.org>
Sent: Thursday, November 01, 2012 9:39 PM
To: Stirling, Bryan
Subject: RE: SCBA - DOR Database Breach

Hey,

I just pulled up the time of the meeting. We had needed 9am or anything after 12. Fred can't do 11am.

Can we work it out?

Thanks,

Neil

From: Stirling, Bryan [BryanStirling@gov.sc.gov]
Sent: Thursday, November 01, 2012 5:59 PM
To: Neil Rashley
Subject: RE: SCBA - DOR Database Breach

Sure. What time?

From: Neil Rashley [mailto:nrashley@scbankers.org]
Sent: Thursday, November 01, 2012 5:59 PM
To: Stirling, Bryan
Subject: Re: SCBA - DOR Database Breach

Could we have a Monday meeting? Fred Green, our new CEO, is out of town until then. FYI he's the former CEO of NBSC and Synovus. Very knowledgeable banker.

Neil

Sent from my iPhone

On Nov 1, 2012, at 4:22 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:
Thank you for your offer and taking time to talk today. I will keep you posted and reach out to you.

From: Neil Rashley [mailto:nrashley@scbankers.org]
Sent: Thursday, November 01, 2012 4:20 PM
To: Stirling, Bryan
Subject: SCBA - DOR Database Breach

Bryan,

Thanks for calling me back. I know this is a constantly evolving situation but we wanted to make sure the Governor's Office used us as one of its primary sources of information for what banks do, especially in these situations. Also, we have been communicating with our bankers and trying to give them the most up-to-date information so they can advise their customers.

So, here's our points:

- Please use us as the primary source for the Governor's Office on what banks do and what they can offer.
- Keep us updated as to the extent of taxpayers' bank account information that has been accessed.
- If there is any way we can assist in helping you inform the public, then we will help.
- You mentioned a meeting and we would like to meet as soon as possible.

Thanks and contact me at any time.

Neil Rashley
Senior Vice President and Counsel
South Carolina Bankers Association
2009 Park Street
P.O. Box 1483
Columbia, SC 29202
(803) 779-0850
(803) 467-221 (cell)
(803) 256-8150 (fax)
nrashley@scbankers.org<mailto:nrashley@scbankers.org>
www.scbankers.org<http://www.scbankers.org>

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Friday, November 02, 2012 10:42 AM
To: Stirling, Bryan
Subject: Re: From Greg Young, re: Stats for 11-2-12, 6:30 am PST

You saw those numbers for visits were for Thursday, correct?

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

Sent by my iPhone

On Nov 2, 2012, at 7:23 AM, "Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

Thank you for this info.

From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, November 02, 2012 09:50 AM
To: Stirling, Bryan
Cc: Ozzie Fonseca <ofonseca@experianinteractive.com<mailto:ofonseca@experianinteractive.com>>; Anel Nevarez <Anel.Nevarez@experianinteractive.com<mailto:Anel.Nevarez@experianinteractive.com>>; Jon Neiditz <Jon.Neiditz@nelsonmullins.com<mailto:Jon.Neiditz@nelsonmullins.com>>; Michael Bruemmer <Michael.Bruemmer@experianinteractive.com<mailto:Michael.Bruemmer@experianinteractive.com>>
Subject: From Greg Young, re: Stats for 11-2-12, 6:30 am PST

Bryan, et al.

New numbers for 11-2-12, 6:30 am PST

Total calls: 665,000
Average wait time: 15 min
Total Registrations: 561,000
Number of visits to registration page: approx. 122,00 for FRIDAY ALONE. I do not have cumulative stats at this time, but hope to extract that early next week.

Best,

GY

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services

535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com<mailto:greg.young@experianinteractive.com>

freecreditreport.com<http://freecreditreport.com>
freecreditscore.com<http://freecreditscore.com>
creditreport.com<http://creditreport.com>
protectmyid.com<http://protectmyid.com>
safetyweb.com<http://safetyweb.com>

Stirling, Bryan

From: Greg Young <Greg.Young@experianinteractive.com>
Sent: Friday, November 02, 2012 10:41 AM
To: Stirling, Bryan
Cc: Ozzie Fonseca; Anel Nevarez; Jon.Neiditz@nelsonmullins.com; Michael Bruemmer
Subject: Re: From Greg Young, re: Stats for 11-2-12, 6:30 am PST

122,000 visits

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

Sent by my iPhone

On Nov 2, 2012, at 7:23 AM, "Stirling, Bryan" <BryanStirling@gov.sc.gov<mailto:BryanStirling@gov.sc.gov>> wrote:

Thank you for this info.

From: Greg Young [mailto:Greg.Young@experianinteractive.com]
Sent: Friday, November 02, 2012 09:50 AM
To: Stirling, Bryan
Cc: Ozzie Fonseca <ofonseca@experianinteractive.com<mailto:ofonseca@experianinteractive.com>>; Anel Nevarez <Anel.Nevarez@experianinteractive.com<mailto:Anel.Nevarez@experianinteractive.com>>; Jon Neiditz <Jon.Neiditz@nelsonmullins.com<mailto:Jon.Neiditz@nelsonmullins.com>>; Michael Bruemmer <Michael.Bruemmer@experianinteractive.com<mailto:Michael.Bruemmer@experianinteractive.com>>
Subject: From Greg Young, re: Stats for 11-2-12, 6:30 am PST

Bryan, et al.

New numbers for 11-2-12, 6:30 am PST

Total calls: 665,000
Average wait time: 15 min
Total Registrations: 561,000
Number of visits to registration page: approx. 122,00 for FRIDAY ALONE. I do not have cumulative stats at this time, but hope to extract that early next week.

Best,

GY

Greg Young, APR
Director
Public Relations/Consumer Engagement

Experian Consumer Services
535 Anton, suite 100
Costa Mesa, CA 92626
Direct: 949-567-3791
Mobile: 949-294-5701
greg.young@experianinteractive.com<mailto:greg.young@experianinteractive.com>

freecreditreport.com<http://freecreditreport.com>
freecreditscore.com<http://freecreditscore.com>
creditreport.com<http://creditreport.com>
protectmyid.com<http://protectmyid.com>
safetyweb.com<http://safetyweb.com>

Stirling, Bryan

From: Jeff Stibel <jstibel@dandb.com>
Sent: Friday, November 02, 2012 3:53 PM
To: Stirling, Bryan
Cc: Judy Hackett; Aaron Stibel
Subject: Re: SC

Thanks Bryan. We will dig in ASAP and make sure we work on this. Just so you (and Frank) knows, we worked around the clock to provide SC with a free offer and have never done that before. As a result, there are some system anomalies such as normally we have paying customers who have a username and password. That said, it is all just messaging changes because you can sign up for free to get the username and password so I suspect it is just poorly worded given how quickly it went up. We will get all over this.

Jeff

Jeffrey M. Stibel
Chairman and CEO

Dun & Bradstreet
CREDIBILITY CORP

www.DandB.com

From: <Stirling>, Bryan <BryanStirling@gov.sc.gov>
Date: Friday, November 2, 2012 12:42 PM
To: Jeff Stibel <jstibel@dandb.com>
Cc: Judy Hackett <jhackett@dandb.com>, Aaron Stibel <astibel@dandb.com>
Subject: RE: SC

This is from the Small Business Chamber, can ya'll help?

Bryan,
I am finding the D&B site to be difficult to negotiate and the toll free number dropped me twice when I tried to get some help.

The online registration is confusing because it asks you for your email AND a password. Of course, since none of our businesses have registered before, the request for a password will be confusing. I did click on the "forgot your password?" and was taken to a page with a temporary password. So I used that which took me to a page to create a new password. That worked. But the next page says to purchase products with no listing of the D&B CreditAlert service. So I have no idea if I'm signed up or not.

Please let me know if we can get this straightened out. We notified all our members to sign up so I don't like it when it doesn't work.

Thanks,
Frank

From: Jeff Stibel [mailto:jstibel@dandb.com]
Sent: Wednesday, October 31, 2012 6:16 PM
To: Stirling, Bryan
Cc: Judy Hackett; Aaron Stibel
Subject: Re: SC

No problem Bryan. To fully clarify, "for life"is a bit vague so we should be sure that it is life of the product (i.e., we could be out of business in 200 yrs and I can't imagine that product being live then in any event). I just want to make sure no one is seeming disingenuous. But in the spirit of our conversation, our goal is to help these businesses out long term until this problem is resolved.

Best,

Jeff

On Oct 31, 2012, at 3:09 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

> Thank you for doing this for life.
> That's what we told the press.
>
> ---
>
> **From:** Judy Hackett [mailto:jhackett@dandb.com]
> **Sent:** Wednesday, October 31, 2012 6:02 PM
> **To:** Stirling, Bryan; Jeff Stibel; Aaron Stibel
> **Subject:** RE: SC
>
> We can certainly do this for the life of the product. Offering anything for life is an odd thing because we could be talking about 100 years. It might be better for you to come up with a reasonable amount of time. Let us know either way.
>
> Judy Hackett
> Chief Marketing Officer
> Dun & Bradstreet Credibility Corp
> 22761 Pacific Coast Highway
> Malibu, CA 90265
> O: 310-919-2233
> C: 770-337-4869
> F: 310-919-2948
> www.DandB.com
>
> <image001.png>
>
>

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Wednesday, October 31, 2012 2:54 PM
To: Judy Hackett; Jeff Stibel; Aaron Stibel
Subject: RE: SC

I recall someone saying on the phone with the governor that it was for life. Came someone please verify this? We told the press that.

From: Judy Hackett [mailto:jhackett@dandb.com]
Sent: Wednesday, October 31, 2012 5:52 PM
To: Stirling, Bryan; Jeff Stibel; Aaron Stibel
Subject: RE: SC

This is a product we typically charge monthly annually for. Our thinking was that the right amount of time was a year or so. Thoughts?

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

<image002.png>

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Wednesday, October 31, 2012 2:49 PM
To: Jeff Stibel; Aaron Stibel
Cc: Judy Hackett
Subject: Re: SC

If this a for life product? So if I was a SC business would I get this product for life?

From: Jeff Stibel [mailto:jstibel@dandb.com]
Sent: Wednesday, October 31, 2012 04:37 PM
To: Aaron Stibel <astibel@dandb.com>
Cc: Stirling, Bryan; Judy Hackett <jhackett@dandb.com>
Subject: Re: SC

Great. They are in the middle of the announcement now. Be sure to send them a note when the link is live with the URL as a reminder.

On Oct 31, 2012, at 1:35 PM, "Aaron Stibel" <astibel@dandb.com> wrote:

Team:

We will have a simple SC Coming Soon page up on DandB.com/SC in the next few moments.

We can change this page; I just didn't want the Governor's office to announce something without at least a Coming Soon page up.

This page will be replaced with the actual offer page tomorrow night.

-Aaron

Aaron Stibel
SVP, Technology
astibel@dandb.com
(310) 919 - 2214

<image001.jpg>

From: Stirling, Bryan [mailto:BryanStirling@gov.sc.gov]
Sent: Wednesday, October 31, 2012 1:08 PM
To: Jeff Stibel
Cc: Judy Hackett; Aaron Stibel
Subject: RE: SC

Thank you very much!

From: Jeff Stibel [mailto:jstibel@dandb.com]
Sent: Wednesday, October 31, 2012 4:08 PM
To: Stirling, Bryan
Cc: Judy Hackett; Aaron Stibel
Subject: Re: SC

Thanks Bryan - confirmed and approved.

On Oct 31, 2012, at 1:05 PM, "Stirling, Bryan" <BryanStirling@gov.sc.gov> wrote:

As we discussed we'd like this Credit Alert to be available to any business that has filed a tax return from 1998 to the breach date with SC. Please approve, thank you.