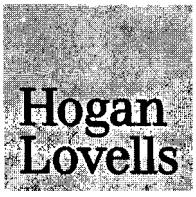

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

March 23, 2012

Attorney General Michael Delaney
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Report of Data Security Incident

Dear Attorney General Delaney:

I am writing on behalf of our client Suddenlink Communications ("Suddenlink") to advise you of a security incident attributable to one of Suddenlink's former employees.

On February 24, 2012, Suddenlink management was notified by law enforcement that a former employee obtained, without authorization, certain personal information of individuals that were employed by Suddenlink and AAT Communications between May 22, 2006 and July 21, 2006. In 2006, Suddenlink Communications and AAT shared human resources functions through their common management company.

Based on the information that we obtained from law enforcement, we believe that the former employee used, or attempted to use, a limited number of individuals' personal information for fraudulent purposes. The investigation uncovered a small number of isolated instances of such use, or attempted use, starting in 2006 and continuing through 2012. The former employee has been arrested and appears to be cooperating with authorities in Overland Park, KS.

The personal information that was obtained by the former employee includes the affected individuals' names, addresses, dates of birth, Social Security numbers, and wage and banking information. For some affected residents, similar information on spouses and dependents was also obtained. At this time, it appears that any misuse of personal information by the former employee was for his own personal benefit, and there is no information to suggest that other individuals were involved. However, at this time we cannot conclusively rule out the possibility that the former employee shared any of the affected individuals' personal information with others.

The former employee obtained the personal information of five New Hampshire residents. Suddenlink is offering two years of identity theft protection services to these individuals. The form of the notice sent to these individuals beginning on March 23, 2012 is attached for your information.

Suddenlink deeply regrets that this incident occurred and is keenly aware of how important it is to safeguard information entrusted to its organization. Suddenlink is taking this matter very seriously and, while Suddenlink has implemented additional controls to improve the security of employee personal information, it will continue to review its security processes and take appropriate actions to minimize the risk of personal information being compromised in the future. Suddenlink has also been working diligently with law enforcement officials to investigate the unauthorized activity and continues to remediate the method of unauthorized access.

If you have any questions about this incident, please do not hesitate to contact me.

Sincerely,

Timothy P. Tobin
Counsel for Suddenlink

Enclosure

March XX, 2012

[Name]
[Address]
[City, State, Zip]

Dear [Name]:

Suddenlink Communications' top priorities include serving the interests of its employees and protecting sensitive information. In keeping with these priorities, we require strict standards in handling employee data; unfortunately however, in late February 2012, we were informed by law enforcement that a former Suddenlink Communications employee had been arrested for alleged illegal use of payroll and benefits information of employees at Suddenlink. Even though we were only recently informed of this incident, the former employee obtained the information from documents taken between May 22, 2006, and July 21, 2006. We sincerely regret that this incident occurred. Below is a summary of what we know about this incident and our suggestions and offer for assistance to help you protect your identity.

What information was included in the documents that were taken?

The non-public personal information that was contained in those documents included your name, address, date of birth, Social Security number, and wage and banking information.

How many people were affected and has my information been used fraudulently?

Based on the information law enforcement provided to us, we believe that the former Suddenlink Communications employee used, or attempted to use, a limited number of individuals' personal information for fraudulent purposes. The investigation uncovered a small number of instances of such use, or attempted use, starting in 2006 and continuing through 2012. **The information given to us by law enforcement indicates that your information was not used, but we still encourage you to be vigilant.** The former employee has been arrested and appears to be cooperating with authorities.

What do I need to do?

Although you may not have had attempts to use your identity, we still encourage you to be vigilant. Experts in identity theft suggest you take the following steps:

1. Obtain and review your credit reports for any accounts or transactions that are not yours. You can obtain your free credit reports at www.annualcreditreport.com. By law, you are eligible to receive one free credit report from each of the three credit bureaus each year.
2. If fraud is discovered, place a fraud alert at one of the three credit bureaus, Equifax, Experian or TransUnion. You would only need to notify one agency and by law they must notify the other two. In the event it is necessary, we have provided the contact information for all three agencies in the attached instructions letter.
3. Review your bank account statements and watch for any future unauthorized activity on your accounts.

What services are Suddenlink providing to assist me?

Because maintaining the security of your personal information is very important to us, and to help safeguard against the possibility of misuse of your personal information, **Suddenlink Communications has arranged for you to receive IDSafeChoice identity theft services through Aon at no cost to you for two (2) years from the date of this letter.** These services include identity theft resolution, internet

fraud monitoring, and up to $25,000 in identity recovery expense reimbursement for any expenses you may incur as a result of recovering from identity theft.

You do not need to do anything to be eligible for the identity recovery services; however, in order to take advantage of the internet monitoring and expense reimbursement insurance you must go online and activate your monitoring services. If you have questions, need help with the placement of fraud alerts, have a suspicion or have seen some evidence of fraudulent activity, contact an Identity Recovery Advocate for assistance between the hours of 8:00am and 5:00pm Eastern at the number shown below. **A complete description of how to activate your internet monitoring services is included in the attached explanation from The Recovery Care Center, your identity theft solutions provider.** The attached instructions for activating your services contains additional information about these services, disclosures regarding the insurance, and provides an access code that allows you to register at no cost. **Please be sure to keep this letter - you will need the access code to register for the services.**

What have you done to improve security since this incident?

Since 2006, Suddenlink Communications has implemented additional controls to improve the security of employee personal information and will continue to review its security processes. Please be assured that Suddenlink is taking this matter very seriously and taking appropriate action to help prevent any recurrence of any incidents like this in the future. We sincerely regret that this incident occurred.

Why did this former employee take the information? Is there anyone else involved?

At this time, it appears that any misuse of personal information by the former Suddenlink Communications employee was for his own personal benefit, and there is no information to suggest that other individuals were involved. However, at this time we cannot conclusively rule out the possibility that some of your personal information was shared with others by the former employee.

What have you been doing since learning of this incident in late February?

Since learning of this incident we have been working diligently with law enforcement officials to investigate the unauthorized activity to identify those individual employees who were possibly affected and to establish a program to assist impacted individuals. **Law enforcement is continuing to put together the case against this former employee.**

If you believe that you have been the victim of identity theft, please contact Det. Byron Pierce of the Overland Park Police Department at 913-344-8703 and 913-344-8704. As mentioned above, you may also contact the Identity Care Hotline number shown below between the hours of 8:00am and 5:00pm Eastern to request the help of an Identity Advocate.

We sincerely regret the inconvenience that this incident may cause you. If you would like further information about the no-cost services offered, need assistance in registering for these services or **if you have other questions, please contact the Identity Care Hotline at 1-800-505-5440 at any time**.

Sincerely,

Suddenlink Communications

The IDSafeChoice Recovery Care Center

You have been provided, at no cost to you, the following services for two years:

1. *Internet monitoring of up to 25 personal credentials for online compromise for one person in the family*
2. *Identity recovery expense reimbursement insurance for up to $25k for the family**
3. *Fully managed identity theft remediation and recovery for the family**

** Family is defined as children under the age of 21 living in the household plus your spouse.*

There is nothing you need to do to be eligible for the identity theft remediation and recovery services. For your protection, you are required to complete a brief enrollment process before we can activate your internet monitoring service and insurance benefits. To complete the enrollment process and activate your internet monitoring, please follow these easy steps:

1. Visit https://aonprotect.merchantsinfo.com
2. Click the **red** "Get Started" button.
3. Click the **red** "Enroll" button on the right had side of the page.
4. You will be prompted to input this promotional code:
5. Enter the required information in "Your Personal Information" section to activate your complimentary benefit and internet monitoring service.

Please Note: There is no cost to you for this service. You are provided with fully managed restoration and internet monitoring services. If you wish to order a copy of your credit report at no cost, please visit www.annualcreditreport.com

If you have any questions regarding your benefit or internet monitoring services or you encounter a problem while enrolling you may call Merchants Information Solutions at 1-800-505-5440 and a representative will be happy to assist you.

Note: Identity theft insurance is underwritten by subsidiaries or affiliates of Chartis Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage that will be provided to your upon your registration. Coverage may not be available in all jurisdictions.

MIS- IRPNXG

Powered By: Merchants

Additional Information

It is important to guard vigilantly for incidents of fraud and identity theft. Even if you do not feel the need to register for the credit monitoring service, we recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

If you are concerned about identity theft you may want to place an alert at each of the three credit reporting agencies. **You need only contact one of these agencies and the information will automatically be provided to the other two.** For your convenience the information for all three agencies is shown below:

Equifax

PO Box 740256
Atlanta, GA 30374
www.equifax.com

To place a **fraud alert**, call 1-800-525-6285 or go to the Equifax Fraud Alert website.

For general info or to request a credit report, call 1-800-685-1111.

To place a **security freeze**, send a written request by regular, certified, or overnight mail to:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com

To place a **fraud alert** through the Experian Fraud Center website.

For general info, to request a credit report, or to place a fraud alert, call 1-888-397-3742.

To place a **security freeze**, send a written request by regular, certified, or overnight mail to:

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union

P.O. Box 1000
Chester, PA 19022
www.transunion.com

To place a **fraud alert**, call 1-800-680-7289, or visit the Trans Union Fraud Alert website.

For general info or to request a credit report, call 1-800-888-4213.

To place a **security freeze**, send a written request by regular, certified, or overnight mail to:

Trans Union Security Freeze
Fraud Victim Assistance Dept.
P.O. Box 6790
Fullerton, CA 92834

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your bills, account statements and credit reports, and promptly report any fraud, suspicious activity, or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW,
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

You may obtain information from the FTC and the consumer reporting agencies listed above about fraud alerts and security freezes. We also provide some additional information about fraud alerts and security freezes below.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud

alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below. Once you have requested an alert with one agency, your request will be automatically sent to the other two agencies. In most cases, the alert will be placed on your credit file with all three agencies within 48 hours.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. ***Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*** To place a security freeze on your credit report, you must send a written request with the following information to **each** of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses listed below. However, since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies at the numbers above to find out more information.

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, the addresses where you lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued ID card (state driver's license or ID card, military ID, etc.);
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

For North Carolina Residents:
If you are a North Carolina resident, you may contact the North Carolina Attorney General's Office to obtain additional information about preventing identity theft.

North Carolina Attorney General's Office, Consumer Protection
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, www.ncdoj.gov

For Maryland Residents:
If you are a Maryland resident, you may contact the Office of Attorney General to obtain additional information about preventing identity theft.

Office of Attorney General of Maryland
200 St. Paul Place, Baltimore, MD 21202, 410-576-6491 or 1-888-743-0023 (toll-free in Maryland),
www.oag.state.md.us/idtheft/index.htm
idtheft@oag.state.md.us