March 6, 2016

2550 Denali St., Suite 1000
Anchorage, AK 99503

JOHN Q. SAMPLE
123 MAIN STREET
ANYWHERE, AK 99501

NOTICE OF DATA BREACH

Privacy and security are priorities at GCI so I am deeply sorry to report to you that on March 3, 2016, we discovered employee W-2 information had been disclosed to an outside party in an email phishing attack.

Our interdepartmental security incident response team has reported this incident to law enforcement, but the reality is that the information is not retrievable. The team and management are working together to pursue every opportunity to mitigate the impact of the incident and protect our employees and past employees.

What Happened?

In February 2016, our payroll department was targeted by a phishing attack. Working through email, a third party impersonated our chief financial officer and requested employee payroll information, specifically copies of the W-2 Wage and Tax Statement forms for everyone who worked for GCI during calendar year 2015.

The employee who received the sham email correctly questioned the request as unusual. The third party impersonating our chief financial officer persisted with the request, however, and ultimately the requested information was emailed to the third party on February 24, 2016.

I want to be clear here. This "social engineering" attack did not compromise any of GCI's IT systems or networks. Nor did it expose any GCI customer information.

Who Was Affected?

We believe that the 2015 W-2s of all employees who worked for GCI, Denali Media, UUI, and Unicom at any time between January 1, 2015 and December 31, 2015 have been disclosed.

What Information Was Involved?

Each W-2 includes the employee or past employee's: (i) Social Security number, (ii) name and address, and (iii) 2015 income and tax withholding information. The W-2 does not include any credit card or bank account information.

What We Are Doing

Immediately after learning of the attack, the security incident response team interviewed the relevant GCI employees, collected and preserved electronic evidence, and notified the FBI. The team is continuing to investigate the attack. As further described below, we have also engaged a well-reputed credit service company, AllClear ID, to provide each affected individual with two-years of free credit monitoring, identity theft counseling and other services, and identify-theft insurance.

The GCI management team takes this attack very seriously. We are moving to further strengthen the protection of employee information and launch an already-planned anti-phishing training program. We will also continue to reinforce our overall privacy and security posture.

What You Can Do

The perpetrators of the phishing attack are most likely motivated by money. They could use the W-2 information to file fraudulent federal income tax returns. They could also use the W-2 information to fraudulently acquire credit cards or other commercial benefits. Here are some specific ways you can mitigate these risks:

- IRS Notification. To minimize the risk of tax fraud, we strongly recommend that you notify the IRS that your tax year 2015 W-2 has been compromised by (i) completing IRS Form 14039 (https://www.irs.gov/pub/irs-pdf/f14039.pdf) and (ii) mailing or faxing the completed form to the IRS. (IRS procedures do not allow GCI to file a single form covering all GCI employees.) **Attachment A** to this letter includes important information on this process and a copy of the form is included at the end of this packet.

  After filing the form, you will likely receive a personal identification number (PIN) from the IRS to use in connection with filing your tax return for tax year 2016. However, you should proceed to file any returns due for tax year 2015 in the normal manner and at the appropriate time.

- Credit Monitoring & Related Services. As an added precaution, we have arranged to have AllClear ID protect your identity for two years at no cost to you. The following identity protection and credit monitoring services start on the date of this notice, and you can use them at any time during the next two years.

  AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-877-676-0379 and a dedicated investigator will do the work to recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

  AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling toll-free at 1-877-676-0379 using the following redemption code: **REDEMPTION CODE**. Additional terms of service related to AllClear's service are included as **Attachment B**.

- In-House Help. GCI's HR team has set up a dedicated email address to respond to any questions or concerns you may have at employeeinfo@gci.com. You can also call HR at (907) 868-5422. This dedicated email address and phone number are available to current and past employees receiving this notice. For current employees, the security incident response team is creating an Intranet page to post status updates and information about protecting yourself from phishing and other fraudulent online activity, and we will provide this information to past employees, upon request.

To protect against possible fraud, identity theft, or other financial loss, we strongly recommend that you remain vigilant, review your account statements, and monitor your credit reports to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity. **Attachment C** contains more information about steps you can take to protect yourself against fraud and identity theft. If you have questions about how to protect yourself from having your information used fraudulently, you can call AllClear ID at 1-877-676-0379.

We apologize for the inconvenience and anxiety this situation may cause you and your family and assure you that we are doing our best mitigate the consequences.

Sincerely,

Greg Chapados
Executive Vice President and Chief Operating Officer

ATTACHMENT A

As explained above, we strongly recommend that you notify the IRS that your tax year 2015 W-2 has been compromised by filing IRS Form 14039 (available online at https://www.irs.gov/pub/irspdf/f14039.pdf). We have attached the form to the end of this packet.

Instructions for filling out IRS Form 14039:

- We have checked the appropriate box and pre-filled the explanatory information in Section A. This form will work regardless of whether you are or were employed by Denali Media, GCI, Unicom, or UUI.

- You should fill out Sections B, C, D, E (only if applicable), and F, then mail or fax the form to the IRS at the address or fax number listed on the form.

- As specified in Section D of the form, the form must be accompanied by a photocopy of the employee's driver's license or other type of identification specified on the form.

After filing the form, you will likely receive a personal identification number (PIN) from the IRS to use in connection with filing your income tax return for tax year 2016. However, you should proceed to file any returns due for tax year 2015 in the normal manner and at the appropriate time.

ATTACHMENT B

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by GCI.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from GCI (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from GCI.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Secure, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

ATTACHMENT C

In addition to the services that GCI is providing, you may want to take the following precautions to guard against the misuse of your information. Here are some things you can do that will minimize your risk:

1. Monitor Accounts. Check your monthly credit and bank account statements carefully for suspicious charges, and notify your financial institution of all charges that you do not recognize. Close any accounts that you think have been compromised.

2. Review Credit Reports Regularly. Federal law allows you to request, free of charge, your credit report from each credit reporting agency annually. Contact the credit reporting agencies at the numbers listed below, or you can call toll-free 1-877-322-8228, visit www.annualcreditreport.com, or complete the Annual Credit Report Request Form online and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281 (visit www.annualcreditreport.com for information on getting your free reports).

Equifax	**Experian**	**TransUnion**
(800) 525-6285	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30348	Allen, TX 75013	Fullerton, CA 92834

3. Fraud Alert. Even if you have credit monitoring in place, you can place a fraud alert on your credit card. You may contact any one of the three major credit reporting agencies listed above to place the alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. As soon as one agency confirms your fraud alert, the others are notified to place fraud alerts.

A fraud alert will not prevent access to your credit report, but it will alert the reporting agency and businesses checking on your credit that your information may have been compromised and encourage them to verify your identity. If you elect to place a security freeze on your credit file (as explained below), a fraud alert is not necessary.

4. Security Freeze. You may wish to place a security freeze on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit reporting agencies without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00 each to place, temporarily lift, or permanently remove a security freeze.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

5. Stay Informed. There are several consumer resources available that provide valuable information on identity theft, and how to avoid becoming a victim. The Federal Trade Commission maintains a website that contains a wealth of information on identity theft, including information on fraud alerts and security freezes, at www.ftc.gov/idtheft. You can also can call 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. If you believe that you are a victim of identity theft, we encourage you to report it to the FTC, law enforcement, your state Attorney General, and to the credit agencies.

5. Additional Resources.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; telephone (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; telephone (877) 566-7226; or www.ncdoj.gov.

Form 14039 Rev. February 2014	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

Complete and submit this form if you are an actual or potential victim of identity theft and would like the IRS to mark your account to identify questionable activity.

Check only one of the following two boxes if they apply to your specific situation. (Optional for all filers)

☐ I am submitting this form in response to a mailed notice or letter from the IRS.

☐ I am completing this form on behalf of another person, such as a deceased spouse or other deceased relative. You should provide information for the actual or potential victim in Sections A, B, & D.

Note to all filers: Failure to provide required information on **BOTH** sides of this form **AND** clear and legible documentation will delay processing.

THIS FORM MUST BE SIGNED ON THE REVERSE SIDE (SECTION F).

Section A – Reason For Filing This Form (Required for all filers)

Check only **ONE** of the following two boxes. You **MUST** provide the requested description or explanation in the lined area below.

1 ☐ I am a victim of identity theft **AND** it is affecting my federal tax records.

You should check this box if, for example, your attempt to file electronically was rejected because someone had already filed using your Social Security Number (SSN) or Individual Taxpayer Identification Number (ITIN), or if you received a notice or correspondence from the IRS indicating someone was otherwise using your number.

Provide a short explanation of the problem and how you were made aware of it.

2 ☒ I have experienced an event involving my personal information that may at some future time affect my federal tax records.

You should check this box if you are the victim of non-federal tax related identity theft, such as the misuse of your personal identity information to obtain credit. You should also check this box if no identity theft violation has occurred, but you have experienced an event that could result in identity theft, such as a lost/stolen purse or wallet, home robbery, etc.

Briefly describe the identity theft violation(s) and/or the event(s) of concern. Include the date(s) of the incident(s).

On February 24, 2016, copies of tax year 2015 W-2 forms issued by my employer, GCI Communication Corp and/or one of its affiliates, were stolen in an e-mail phishing attack. My tax year 2015 W-2 was one of the stolen forms.

Section B – Taxpayer Information (Required for all filers)

Taxpayer's last name	First name	Middle initial	The last 4 digits of the taxpayer's SSN **or** the taxpayer's **complete** Individual Taxpayer Identification Number (ITIN)

Taxpayer's **current** mailing address (apt., suite no. and street, or P.O. Box)

City	State	ZIP code

Tax year(s) affected *(Required if you checked box 1 in Section A above)*	Last tax return filed (year) *(If you are not required to file a return, enter NRF and do not complete the next two lines)*

Address on last tax return filed *(If same as current address, write "same as above")*

City (on last tax return filed)	State	ZIP code

Section C – Telephone Contact Information (Required for all filers)

Telephone number *(include area code)* ☐ Home ☐ Work ☐ Cell	Best time(s) to call

I prefer to be contacted in *(select the appropriate language)* ☐ English ☐ Spanish ☐ Other _____

Section D – Required Documentation (Required for all filers)

Submit this completed form and a **clear and legible** photocopy of at least one of the following documents to verify your identity. If you are submitting this form on behalf of another person, the documentation should be for that person. If necessary, enlarge the photocopies so all information and pictures are clearly visible.

Check the box next to the document(s) you are submitting:

☐ Passport ☐ Driver's license ☐ Social Security Card ☐ Other valid U.S. Federal or State government issued identification**

** Do not submit photocopies of federally issued identification where prohibited by 18 U.S.C. 701 (e.g., official badges designating federal employment).

Form 14039 Rev. February 2014	Department of the Treasury - Internal Revenue Service **Identity Theft Affidavit**	OMB Number 1545-2139

Section E – Representative Information (Required only if completing this form on someone else's behalf)

If you are completing this form on behalf of another person, you **must** complete this section **and** attach **clear and legible** photocopies of the documentation indicated.

Check only **ONE** of the following four boxes next to the reason why you are submitting this form

- ☐ The taxpayer is deceased and I am the surviving spouse. *(No attachments are required)*
- ☐ The taxpayer is deceased and I am the court-appointed or certified personal representative. Attach a copy of the court certificate showing your appointment.
- ☐ The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed. Attach a copy of the death certificate or the formal notification from the appropriate government office informing the next of kin of the decedent's death. Indicate your relationship to the decedent: _____
- ☐ The taxpayer is unable to complete this form and I have been appointed conservator or have Power of Attorney (POA) authorization. Attach a copy of the documentation showing your appointment as conservator or your POA authorization. If you are the POA and have been issued a CAF number by the IRS, enter it here: _____

Representative's name

Current mailing address

City	State	ZIP code

Section F – Penalty Of Perjury Statement and Signature (Required for all filers)

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this form is true, correct, complete, and made in good faith.

Signature of taxpayer or representative of taxpayer	Date signed

Instructions for Submitting this Form

Submit this form and **clear and legible** copies of required documentation using **ONE** of the following submission options. Mailing **AND** faxing this form **WILL** result in a processing delay.

By Mail

If you checked Box 1 in Section A and are unable to file your return electronically because the primary and/or secondary SSN was misused, attach this form and documentation to your paper return and submit to the IRS location where you normally file. **If you have already filed your paper return,** submit this form and documentation to the IRS location where you normally file. Refer to the "Where Do You File" section of your return instructions or visit IRS.gov and input the search term "Where to File".

If you checked Box 1 in Section A and are submitting this form in response to a notice or letter received from the IRS, return this form and documentation **with a copy of the notice or letter** to the address contained in the notice or letter.

If you checked Box 2 in Section A (you do not currently have a tax-related issue), mail this form and documentation to:

Internal Revenue Service
PO Box 9039
Andover MA 01810-0939

By FAX

If you checked Box 1 in Section A and are submitting this form in response to a notice or letter received from the IRS that shows a reply FAX number, FAX this completed form and documentation with a copy of the notice or letter to that number. Include a cover sheet marked "Confidential." If no FAX number is shown, follow the mailing instructions on the notice or letter.

If you checked Box 2 in Section A (you do not currently have a tax-related issue), FAX this form and documentation to: **(855) 807-5720.**

NOTE: The IRS does not *initiate* contact with taxpayers by email, fax, or any social media tools to request personal or financial information. Report unsolicited email claiming to be from the IRS and bogus IRS websites to phishing@irs.gov.

NOTE: For more information about questionable communications purportedly from the IRS, visit IRS.gov and input the search term "Fake IRS Communications".

Other helpful identity theft information may be found on www.irs.gov/uac/Identity-Protection. Additionally, locations and hours of operation for Taxpayer Assistance Centers can be found at www.irs.gov (search "Local Contacts").

Note: The Federal Trade Commission (FTC) is the central federal government agency responsible for identity theft awareness. The IRS does not share taxpayer information with the FTC. Refer to the FTC's website at **www.identitytheft.gov** for additional information, protection strategies, and resources.

Privacy Act and Paperwork Reduction Notice

Our legal authority to request the information is 26 U.S.C. 6001.
The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties.
You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103.
Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W:CAR:MP:T:T:SP, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.