November 13, 2017

2550 Denali St., Suite 1000

John Q. Sample
123 Main Street
Anywhere, AK 99501

NOTICE OF DATA BREACH

GCI takes privacy and security seriously. That is why we regret to inform you that we recently learned of a data breach that involved a trusted third party contractor removing files from a GCI server that contained employee names and Social Security numbers.

What Happened?

Last Thursday, November 2, 2017 The Siegfried Group, an outside contract services firm that provides accounting contractors to GCI, notified us that one of its accountants had downloaded a limited amount of GCI data from a restricted folder onto an external drive without permission or authorization to do so. The stolen information included a 2015 GCI report used to track accrued employee vacation amounts and listed employee names and Social Security numbers.

In late September, The Siegfried Group became aware that its employee may have mishandled client data. On October 9 The Siegfried Group employee disclosed that he had downloaded data from several clients onto a personal external drive. Upon discovery of the employee's unauthorized downloading, The Siegfried Group recovered the external drive and initiated an investigation with help from an outside forensic firm. On approximately October 17 The Siegfried Group determined that GCI data was on the external drive. The Siegfried Group notified GCI of the incident on November 2. As a result of his actions, The Siegfried Group fired the employee.

The employee worked for The Siegfried Group on the GCI account from approximately January 2015 to July 2015 and downloaded the GCI data onto the external drive around July 2015. While working at GCI, the employee had limited access to GCI employee records. Although The Siegfried Group employee removed the data from the GCI server without authorization, we have no indication of why he downloaded the information. Additionally, we have no indication of any further misuse or disclosure of the data. Despite this, out of an abundance of caution we immediately wanted to let our employees know about this issue and work to remedy any impact. Importantly, this incident was not the result of a compromise of any of GCI's IT systems or networks nor did it expose any GCI customer information.

Who Was Affected?

We believe that all active GCI employees employed as of June 30, 2015 were affected.

What Information Was Involved?

The information disclosed included your first and last name and Social Security number along with your base compensation and hours of accumulated leave as of June 30, 2015, along with other non-sensitive information. This information did not include your personal address, or any user credentials, credit card or bank account information.

What We Are Doing.

Upon learning of this incident, we immediately began working with The Siegfried Group and their computer forensics firm to understand the details of the incident and identify GCI employees whose information may have been involved. Additionally, we reported the incident to law enforcement and are fully cooperating with them.

We have also decided to extend the free credit monitoring and identification theft protection services that we offered to employees in 2016. This service is also available to those employees who did not previously elect to use the credit monitoring or who may have cancelled the service. Details of those monitoring services can be found below.

The GCI management team takes the security of our employee's information very seriously. We are working with our information security team to enhance our controls to detect and prevent this type of incident in the future. We will also continue to reinforce our overall privacy and security posture internally and with third parties.

What You Can Do.

Based on the information we have received to date, there are no indications that any employees or other individuals have been the victims of identity theft or fraud because of this incident. Despite this, we have listed some specific steps you can take to ensure your information is more secure. If you previously took any of the steps discussed below and did not make any changes, nothing more is required of you. All actions you took and precautions you put in place should still be in effect and continue to provide their benefits.

- Credit Monitoring & Related Services. We have extended the AllClear identify theft protection service that was initially offered in 2016 at no cost to employees for two additional years. If you previously signed up for AllClear the last time it was offered and have not cancelled the service prior to receipt of this letter, you don't need to do anything: the prior service that you selected (including any service your spouse received) has been automatically extended for two years. For those who did not sign up for these credit monitoring services (or previously cancelled the service), we are offering them at no cost for two years. Options include:
    - *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 redemption code provided in March 2016. If you cannot find that code, please contract GCI Human Resources at employee@gci.com or (907) 868-5422.

- *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. Additional terms of service related to AllClear's service are included as **Attachment A**.

- In-House Help. GCI's HR team has set up a dedicated email address to respond to any questions or concerns related to this incident that 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 fraudulent online activity, and we can make this information available to past employees, upon request.

Although we are not currently aware of any indications that any employees have experienced or are likely to experience fraud or identity theft as a result of this incident, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history 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 B** 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.

Additionally, the APD has created a master police report to cover this incident; the APD case number is 17-510405. Credit reporting agencies may ask you for this number when you request certain protections such an extended fraud alert or security freeze.

For More Information.

We apologize for any concern this situation may cause you and your family. If you have any questions about this notice or the incident, please feel free to contact us at (907) 868-5422 or employeeinfo@gci.com.

Sincerely,

Joe Wahl
Chief Human Resource Officer

ATTACHMENT A
AllClear Identity Repair 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:

- Coverage through March 31, 2020 with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

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 Identity Repair 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 through March 31, 2020 (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements

To be eligible for Services under AllClear Identity Repair 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 Identity Repair 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 Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- 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 Identity Repair 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, or
  - 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; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair 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 Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- 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 AllClear Identity Repair 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 Identity Repair, 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 B

Additional Information

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and to place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit http://www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

Consider contacting the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

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.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax:	Experian:	TransUnion:
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
1-888-766-0008	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

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 five (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.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

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

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.