

DEBORAH HOWITT SHINBEIN LLC

2531 XENIA ST. DENVER, CO 80238
OFFICE: (303)997-1325 * CELL: (303)960-6626
DEB@DEBSHINBEIN.COM

November 7, 2013

VIA FEDEX

State of New Hampshire
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Notice of Data Security Breach

To Whom It May Concern:

Please be aware that Clarity Media Group, Inc. has suffered a security breach. A laptop was stolen from the car of a Clarity Media Group subsidiary's employee on October 12, 2013. Although the laptop was password protected and several files were encrypted, we have analyzed the laptop's backup files, and we have come to the conclusion that the laptop contained unencrypted files including personally identifiable information ("PII") regarding current or former employees of Clarity Media Group and its subsidiaries, or of Freedom Communications (the former owner of the Colorado Springs Gazette, which is now owned by Clarity Media Group).

We believe the following PII about some individuals may have been stored in unencrypted form on the laptop: first name, last name, mailing address, email address, phone number, date of birth, social security number, wages, and 401(k) balance. The PII that was the subject of this incident was in electronic form. This PII regarding spouses, children, or other dependents of some of the affected individuals may also have been on the laptop. If PII for any of these individuals was present on the laptop, they will receive a separate letter.

NUMBER OF RESIDENTS AFFECTED AND NOTIFIED

We believe that this incident only affected one individual residing in New Hampshire whose personal information was the subject of the incident. Written notice of this incident was sent to the New Hampshire resident on Nov. 6, 2013 via first class U.S. mail. A copy of the form of notice sent to the affected New Hampshire resident is attached to this letter. Notification to individuals was not delayed due to a law enforcement investigation, but rather was slightly delayed due to our own analysis of the laptop's backup files, to determine what PII regarding which individuals was likely to have been present on the laptop.

STEPS TAKEN RELATING TO THE INCIDENT

When we discovered the breach, it was promptly reported to local law enforcement. However over the course of the next few days, as the backup files for the stolen laptop were located and analyzed, the scope of the breach and the fact that there was likely unencrypted PII on the laptop, was discovered. We do not have any evidence that the PII has been used for fraudulent purposes, and accordingly, Clarity Media Group does not plan to credit morning services to all impacted individuals. However, it will consider offering such services on a case by case basis.

Clarity Media group has taken all available measures to remotely disable the laptop from accessing any company networks. The theft was promptly reported to local law enforcement and the company will continue to work with them as requested. In addition, Clarity Media Group has begun implementing a new security plan to minimize the risk of another breach in the future.

CONTACT INFORMATION

If you have any questions, you may contact me at the number/email above, or contact:

Bob Manzi, Controller
Clarity Media Group
(303)299-1506
bmanzi@claritymg.com
555 17th St., Suite 700
Denver, CO 80202

Please let us know if you require any further information.

Best regards,



Deborah Shinbein
Principal, Deborah Howitt Shinbein, LLC

cc: Bob Manzi, Clarity Media Group

November 5, 2013

[INSERT ADDRESS]

Re: Security Breach Involving Your Personal Information

Dear _____.

We are writing to you because of a recent security breach regarding personal information of many current or past employees of Clarity Media Group (“Clarity”) and its subsidiaries, including former employees of The Gazette under prior ownership, and other former employees of Freedom Communications. If you are receiving this letter, it means that following our investigation, we believe that your personal information was on a stolen laptop, as further described below.

What happened?

A laptop was stolen from the car of a Clarity Media Group subsidiary’s employee on October 12, 2013. We have analyzed the laptop’s backup files, and we have come to the conclusion that the laptop contained unencrypted files including personally identifiable information (“PII”). Although the laptop itself was password protected, we believe the following PII about some individuals may have been stored in unencrypted form on the laptop: first name, last name, mailing address, email address, phone number, date of birth, social security number, wages, and 401(k) balance. This PII regarding spouses, children, or other dependents of some of the affected individuals may also have been on the laptop. If PII for any of these individuals was present on the laptop, they will receive a separate letter. Although we cannot determine exactly which elements of your PII may have been on the laptop, you should assume that any of the PII described above may have been compromised.

What are the risks of this information being used?

Because the laptop was stolen from a car in a parking lot, we have no way of knowing what the thief intends to do with the laptop or the data stored on the laptop, or how sophisticated the thief may be with regard to accessing the laptop’s data.

What is Clarity doing to protect your interests?

- We have taken all available measures to remotely disable the laptop from accessing any company networks;
- We have notified law enforcement authorities and we will continue to work with them as requested;
- We are notifying individuals who may have had information on the laptop, so that they can take appropriate steps to protect themselves against credit card fraud and identity theft; and

- We have begun implementing a new security plan to minimize the risk of another breach in the future.

What steps can I take to protect myself?

To protect yourself from the possibility of identity theft or other fraud, we recommend that you place a 90 day Fraud Alert on your credit file. The fraud alert helps to prevent someone else obtaining credit in your name. If you have a fraud alert on your credit file, creditors will contact you and verify your identity before they open any new accounts or change your existing accounts, but it should not affect your credit score or your ability to obtain new credit (although it may cause a delay in any applications or approvals). As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts, so you do not need to place alerts with more than one of the credit bureaus. To place a fraud alert, go to any of the following links and complete the requested steps:

<https://www.experian.com/fraud/center.html>

[https://www.alerts.equifax.com/AutoFraud Online/jsp/fraudAlert.jsp](https://www.alerts.equifax.com/AutoFraudOnline/jsp/fraudAlert.jsp)

<http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page>

If you have reason to be extremely concerned about the possibility of identity theft, you may also wish to institute a security freeze on your credit file, which is a more lengthy process. See the attached Resources page for more details.

In addition, you may wish to obtain a free credit report from any or all of the three credit bureaus, to ensure that no accounts have been opened in your name at this time. The main contact information for each credit bureau is below:

<p>Equifax 800-525-6285 www.equifax.com</p> <p>P.O. Box 740241 Atlanta, GA 30374-0241</p>	<p>Experian 888-397-3742 www.experian.com</p> <p>P.O. Box 9532 Allen, TX 75013</p>	<p>TransUnion 800-680-7289 www.transunion.com</p> <p>Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790</p>
---	---	---

Even if you do not find any suspicious activity on your initial credit reports, we urge you to remain vigilant in reviewing your account statements and monitoring your credit reports for the next few years. The Federal Trade Commission (FTC) recommends that you check your credit reports periodically because victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly. You may also want to sign up for a credit monitoring program. Although we have never used this program and cannot guarantee any results, one (apparently free) program is available at www.creditkarma.com. Numerous other monitoring programs are also available from third parties.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local police department and file a police report, and contact the State Attorney General for the state in which you reside. Get a copy of any police report or other report you file, as many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.consumer.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Please also notify Clarity at 303-299-1504 after you have notified law enforcement.

For more information about identity theft and how you can reduce the likelihood that your identity will be stolen, see the attached Resources page.

What if I have questions about this breach?

If you have any questions, please send an email to Bob Manzi, Clarity Media Group Controller, at bmanzi@claritymg.com or call Clarity at 303-299-1504.

We deeply regret this incident and apologize to you for the inconvenience it may cause you.

Sincerely,

Ryan McKibben
CEO
Clarity Media Group

RESOURCES

Security Freeze: If you wish to take more extensive measures to prevent new credit being opened in your name, you may consider placing a security freeze on your credit file. You should only place a security freeze if you want to prevent most parties from obtaining your credit report and prevent all credit, loans and related services from being approved in your name without your consent. Please consider that this may also impact or delay your ability to obtain certain government services, rental housing, employment, cell phone plans, insurance, utilities, and many more aspects of your life. You will need to apply for a security freeze separately with each of the credit bureaus. The requirements to obtain a security freeze vary depending on your state of residence, and you may be required to pay a fee, provide detailed identification records (including copies of government issued IDs and utility bills), provide an incident report if you are a victim of identify theft, or take other measures as described on the credit bureaus' websites. You can find more information regarding a security freeze at the following links, or by calling each of the credit bureaus at the numbers listed in the notification letter:

<https://www.freeze.equifax.com>

https://www.experian.com/consumer/security_freeze.html

<http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page>

Federal Trade Commission: The FTC's website at www.consumer.gov/idtheft has information for victims or potential victims of identify theft. You can also obtain this information from the FTC at:

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

Many State Attorney General websites also have information applicable to victims of identity theft in their state. Selected AG offices are provided below.

Residents of Maryland: You can obtain information regarding prevention of identity theft from the FTC or your state attorney general's office:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023

www.oag.state.md.us

Residents of North Carolina: You can obtain information regarding prevention of identity theft from the FTC or your state attorney general's office:

North Carolina Department of Justice
Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
(877)566-7226
www.ncdoj.com

Residents of Iowa: You may report suspected incidents of identity theft to local law enforcement or your Attorney General:

Office of the Attorney General
1305 E. Walnut St.
Des Moines, IA 50319
(515)281-5164
www.iowa.gov/government/ag