GT GreenbergTraurig

Lori S. Nugent
Tel 214.665.3600
Fax 214-665-3601
nugentl@gtlaw.com

June 24, 2015

Attorney General Joseph Foster
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General Foster:

We represent Genius Central ("GC") with respect to an incident involving the exposure of certain personal information described in detail below. This letter supplements the preliminary notice that we provided to Vermont Assistant Attorney General Ryan Kriger on June 2, 2015, which we understand was circulated to the other state attorneys general.

GC is a technology company that provides Internet marketing solutions and business analytics to companies in the natural and health food industry, including the maintenance of websites for such companies. Unfortunately, it appears that the personal information of certain GC clients may have been exposed. At this time, there is no indication that any of the personal information has been misused. Nevertheless, GC has hired Kroll, a global leader in risk mitigation and response, to provide impacted individuals with one year of single bureau continuous credit monitoring and identity theft consultation and restoration services at no cost to the individuals.

1. Nature of the security breach, unauthorized use or access

GC noticed that part of its network was running slower than normal, and immediately investigated the situation. It was determined that assistance from a forensic computer consultant was prudent. During the investigation, on May 12, 2015, the computer consultant determined that malware was installed on GC's system on or about January 9, 2015, which may have exposed social security information pertaining to 256 individuals. It is possible, however, that some information was accessible since October 2014. Further investigation took place to determine whether the social security numbers that may have been exposed were associated with specific individuals' names. While names were not always directly associated with a social security number, when the data was viewed in context, certain names, business contact information, and business e-mail addresses were near what appeared to be a social security number. Significant analysis and data manipulation was required to determine whether valid social security numbers, rather than company tax identification numbers, were contained in the exposed data set. In addition, because GC only had the contact information of the impacted individuals' businesses, GC was required to manually search several different public records databases and cross reference the information obtained to determine each impacted individual's last known mailing addresses. Within three days of obtaining residential mailing addresses, GC began providing notification to state attorneys general, and Kroll anticipates that notification to the impacted population will begin on Friday, June 26, 2015.

While GC encrypts database fields designed to contain credit card information, on June 2, 2015, GC learned that certain credit card information was located in free form text fields that were not encrypted. Specifically, rather than using the designated boxes to submit credit card information, 15 of the impacted individuals entered their credit card information into narrative boxes that customers typically use submit questions or comments. The exposed credit card information may have included name, address, phone number, e-mail address, credit card number, CVV code, and expiration dates.

2. Number of New Hampshire residents affected

Only two (2) New Hampshire residents were affected by the unauthorized exposure. A notification letter will be sent to the affected individuals on June 26, 2015 via regular mail. Copies of both notification form letters are included with this letter.

3. Steps taken and plans relating to the incident

Immediately upon learning of this situation, GC took several steps to close the security vulnerability. In addition to retaining a highly-regarded independent forensic investigation firm to preserve evidence and analyze its system, GC deleted the infected files and disabled the malware. In addition, GC downloaded additional antivirus software, scanned the system, and completely rebooted the system.

GC also has taken steps to prevent this type of event from happening again, including deleting the social security numbers and unencrypted credit card numbers from its system, changing the passwords on the impacted device and all similar devices, increasing the frequency of internal and external security checks, increasing monitoring, and applying other enhanced security controls.

GC has hired Kroll to provide impacted individuals with one year of continuous credit monitoring and identity theft consultation and restoration services at no cost to the individuals. GC also has established a dedicated toll-free number to answer impacted individuals' questions about this incident.

4. Contact information

Notification has been provided to the Consumer Reporting Agencies. If you have any additional questions, please contact me at nugentl@gtlaw.com or 214-665-3630.

Best regards,

Lori S. Nugent

cc: Stephanie A. Reiter, Greenberg Traurig
Tyler Parramore, Genius Central

GeniusCentral™

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a recent security incident that may have resulted in the exposure of your personal information. Genius Central noticed that part of its network was running slowly, and immediately investigated the situation. The investigation determined that there may have been unauthorized access to your name, address, phone number, e-mail address, credit card number, CVV code, and expiration date. We apologize for any inconvenience this situation may cause you. We have hired Kroll, a global leader in risk mitigation and response, to provide you with identity theft protection services including credit monitoring and identity theft consultation and restoration services at no cost to you for one year. Additional information describing your services is included with this letter.

Visit <<IDMonitoringURL>> and follow the online instructions
to take advantage of your Identity Theft Protection Services.

Membership Number: <<Member ID>>

In addition to signing up for identity theft protection services, the attached reference guide provides identity protection suggestions that may be useful to you.

What Happened?

We noticed that part of our system was running slowly, and as we investigated, we determined that assistance from a forensic computer consultant was necessary. During the investigation, on May 12, 2015, the computer consultant determined that malware was installed on our system on or about January 9, 2015, although it is possible that information was accessible since October 2014. While we encrypt fields designed to contain credit card information, on June 2, 2015, we learned that certain credit card information, including yours, was located in unencrypted free form text fields that were available for comments. There is no indication that your information has been misused. Nevertheless, we are sending this letter so that you are aware of this situation, and to provide you with identity theft protection services.

What Steps Have Been Taken?

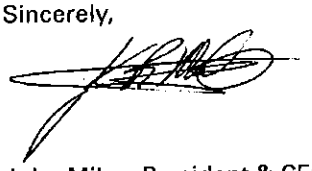
Immediately upon learning of this situation, we took several steps to close the security vulnerability. We deleted the infected files and disabled the malware. In addition, we downloaded additional antivirus software, scanned the system, and completely rebooted the system. We also have taken steps to prevent this type of event from happening again, including deleting the credit card information in free form text fields from our system, changing the passwords on the impacted device and all similar devices, increasing the frequency of internal and external security checks, increasing monitoring, and applying other enhanced security controls.

We have established a dedicated toll-free number that you can call Monday through Friday from 8:00 am - 5:00 pm CST if you have any questions related to this incident. The number to call is 1-???-???-????. ***Please have your membership number ready.***

2232 5th Avenue South, St. Petersburg, FL 33712 | p +800.360.2231 | f +941.480.1720 | www.GeniusCentral.com

We sincerely regret any inconvenience or concern this situation may cause.

Sincerely,



John Miles, President & CEO
GeniusCentral, Inc.

<<IDMonitoringURL>> ***Is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.***
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-???-???-????.

State Notification Requirements

All States.
You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
1-800-888-4213
Chester, PA 19022 www.transunion.com

For residents of Massachusetts.
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.
You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland and North Carolina.
You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

GeniusCentral™

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a recent security incident that may have resulted in the exposure of your personal information. Genius Central noticed that part of its network was running slowly, and immediately investigated the situation. The investigation determined that there may have been unauthorized access to your name, business contact information, e-mail address, and Social Security number. We apologize for any inconvenience this situation may cause you. We have hired Kroll, a global leader in risk mitigation and response, to provide you with identity theft protection services including credit monitoring and identity theft consultation and restoration services at no cost to you for one year. Additional information describing your services is included with this letter.

Visit krollbreach.idMonitoringService.com and follow the online instructions to take advantage of your Identity Theft Protection Services.

Membership Number: <<Member ID>>

In addition to signing up for identity theft protection services, the attached reference guide provides identity protection suggestions that may be useful to you.

What Happened?

We noticed that part of our system was running slowly, and as we investigated we determined that assistance from a forensic computer consultant was necessary. During the investigation, on May 12, 2015, the computer consultant determined malware was installed on our system on or about January 9, 2015, although it is possible that information was accessible since October 2014. Further investigation took place to determine whether the Social Security numbers that may have been exposed were associated with specific individuals' names. While names were not always directly associated with a Social Security number, when the data was viewed in context, your name was near what appeared to be a Social Security number. There is no indication that your information has been misused. Nevertheless, we are sending this letter so that you are aware of this situation, and to provide you with identity theft protection services.

What Steps Have Been Taken?

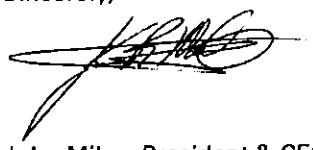
Immediately upon learning of this situation, we took several steps to close the security vulnerability. We deleted the infected files and disabled the malware. In addition, we downloaded additional antivirus software, scanned the system, and completely rebooted the system. We also have taken steps to prevent this type of event from happening again, including deleting the Social Security numbers from our system, changing the passwords on the impacted device and all similar devices, increasing the frequency of internal and external security checks, increasing monitoring, and applying other enhanced security controls.

We have established a dedicated toll-free number that you can call Monday through Friday from 8:00 am - 5:00 pm CST if you have any questions related to this incident. The number to call is 1-866-775-4209. *Please have your membership number ready.*

2232 5th Avenue South, St. Petersburg, FL 33712 | p +800.360.2231 | f +941.480.1720 | www.GeniusCentral.com

We sincerely regret any inconvenience or concern this situation may cause.

Sincerely,



John Miles, President & CEO
GeniusCentral, Inc.

krollbreach.idMonitoringService.com is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. To receive credit services by mail instead of online, please call 1-866-775-4209.

State Notification Requirements

All States.
You may obtain a copy of your credit report or request information on how to place a fraud alert or security freeze by contacting any of the national credit bureaus below. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Equifax
P.O. Box 740241
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2104
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
1-800-888-4213
Chester, PA 19022 www.transunion.com

For residents of Massachusetts.
It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts and West Virginia.
You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent.

To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The consumer reporting agency may charge a fee of up to $5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.
State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission.

For residents of Illinois, Maryland and North Carolina.
You can obtain information from the Federal Trade Commission, and for residents of Maryland and North Carolina, from your respective state Office of the Attorney General, about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

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

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Kroll

Take Advantage of Your Identity Theft Protection Services

You've been provided with access to services from Kroll, a global leader in risk mitigation. Over the past 14 years, Kroll has provided data breach response services for cases impacting more than 100 million individuals including personal consultation to more than 180,000 consumers and worked some 8,000 confirmed identity theft cases. When you need assistance, rest assured that your services are backed by an expert team who can answer any question you may have.

The following services are included in your **Credit Monitoring** package:

Kroll employs a team of experienced licensed investigators to provide you with expert, one-on-one assistance:

Consultation: You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes best practice tips to assist in ongoing protection, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Restoration: Kroll's restoration services are the most comprehensive of any provider. Should you become a victim of identity theft, a dedicated licensed investigator can work on your behalf to resolve related issues. The investigator does more than shoulder the bulk of the recovery; they can dig deep to uncover all aspects of the theft, and then work with creditors, collection agencies, utilities, government entities, and more ... to resolve it.

Credit Monitoring: Credit monitoring can be a key tool in detecting early warning signs of identity theft. You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft. You'll also receive "no activity" notices if there have been no changes to your data.

How to Take Advantage of Your Identity Theft Protection Services

Visit krollbreach.idMonitoringService.com and follow the online instructions to take advantage of your identity theft protection services.

You can view your services at any time by logging onto Kroll's identity protection website. When you enroll, be prepared to provide the membership number included with the accompanying letter.

Help is only a phone call away.

If you have a question, need assistance, or feel you may be a victim of identity theft, call Kroll at the toll-free number provided in the accompanying letter, and ask to speak with an investigator.

Take advantage of this no-cost opportunity and let the experts at Kroll help you assess your situation and safeguard your identity.

krollbreach.idMonitoringService.com is compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox or Safari.