CLARK HILL

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999

clarkhill.com

Jason M. Schwent
T 312.985.5939
F 312.517.7573
Email: jscwent@clarkhill.com

May 15, 2020

Via email – attorneygeneral@doj.nh.gov
Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302
attorneygeneral@doj.nh.gov

To Attorney General MacDonald:

We represent D'Amore Tatman Group, LLC ("D'Amore") as outside counsel with respect to a data security incident involving the potential exposure of certain personally identifiable information ("PII") described in more detail below. D'Amore is a full-service Certified Public Accountant, tax, and strategic business consulting firm. D'Amore is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On February 12, 2020, D'Amore learned of suspicious activity associated with one of its corporate employee email accounts. D'Amore engaged independent computer forensic experts to assist with its investigation. The forensic investigation found that an unauthorized actor appears to have accessed one of D'Amore's corporate employee email accounts through a phishing email attack. The phishing email contained a malicious link, which once clicked, took the employee to an illegitimate log-in screen where the employee's credentials, username and password, were entered and then stolen. While the investigation did show evidence of access to the one corporate email account, the forensic investigators were unable to identify what emails or attachments may have actually been viewed. D'Amore engaged a vendor to conduct a comprehensive review of the one employee's mailbox to determine what PII may have been present in the account, and to extract any contact information for impacted individuals. The review concluded on April 10, 2020, and D'Amore determined that names, addresses, Social Security numbers, and financial account information were found in the account.

2. Number of residents affected.

One (1) New Hampshire residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on May 15, 2020 (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

D'Amore took steps to address this incident and prevent similar incidents in the future. D'Amore enabled multi-factor authentication for all of its email accounts, increased its spam filters, and is currently retraining its staff on cybersecurity and recognizing and responding to suspicious emails. D'Amore also implemented a global password reset. Affected individuals were offered 12 months of credit monitoring and identity protection services through ID Experts.

4. Contact information.

D'Amore takes the security of the information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Very truly yours,

CLARK HILL

JASON M. SCHWENT

Cc: Logan Parker

Enclosure

D'AMORE TATMANGROUP LLC
Certified Public Accountants & Business Advisors

C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 579-1095
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

May 15, 2020

Notice of Security Incident

Dear <<First Name>> <<Last Name>>,

D'Amore Tatman Group, LLC ("D'Amore") recently experienced a data security incident that may have impacted your personal information. D'Amore is a certified public accounting, tax, and strategic business consulting firm. We take the privacy and security of your information seriously, and we sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and the resources we are making available to help you.

What happened?

On January 28, 2020, we learned of suspicious activity associated with one of our corporate email accounts, and engaged independent computer forensic experts to assist us with our investigation. The forensic investigation determined that an unauthorized actor gained access to one corporate email account, but were unable to identify what emails or attachments may have been viewed by the unauthorized actor. We then engaged a vendor to conduct a comprehensive review of the one email account to determine what personal information may have been present in the account. On April 10, 2020, we determined that your personal information may have been stored in the account. Although we have no evidence that your information has been misused, we wanted to let you know about this incident out of an abundance of caution.

What information was involved?

Information such as your name, Social Security number, and financial account information may have been contained in the account.

What we are doing?

We want to assure you that we are taking steps to prevent this type of incident from happening in the future. We have enabled multi-factor authentication for remote access to all email accounts, increased our spam filters, and are currently rolling out an all-employee training program on cybersecurity and recognizing and responding to suspicious emails. We also implemented a global password reset.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What you can do?

We encourage you to contact ID Experts® with any questions and to enroll in free MyIDCare services by calling (833) 579-1095 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is August 18, 2020.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. It is always a good idea to review and monitor your credit card and bank statements and immediately report suspicious activity to your financial institution.

For more information:

If you have any questions or concerns, please call (833) 579-1095 Monday through Friday from 8 am – 8 pm Central Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

D'Amore Tatman Group LLC

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided. Monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact (833) 579-1095 to gain additional information about this event and speak with an ID Experts agent about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.