

Melissa K. Ventrone
312 580 2219 direct
mventrone@thompsoncoburn.com

STATE OF NH
DEPT OF JUSTICE
2018 FEB - 8 AM 10:40

February 2, 2018

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Dear Attorney General Foster:

We represent DiFilippo Corporate Finance Group, Inc. ("DCFG") with respect to a recent data security incident involving the potential exposure of personally identifiable information described in more detail below. DCFG is a professional services firm providing third-party independent valuation and transaction opinions, located in Newburyport, Massachusetts.

1. Nature of security incident.

On December 14, 2017, DCFG discovered suspicious activity involving an employee's email account. DCFG took immediate steps to secure the account and hired an independent computer forensic firm to assist with investigating this matter. On January 12, 2018, the forensic investigation determined that an unauthorized user gained access to the email account through a phishing attack and may have been able to open and download emails between December 5 and December 14, 2017. DCFG conducted a detailed review of the impacted account and determined that a small number of clients' name and Social Security number were contained in an email attachment.

2. Number of New Hampshire residents affected.

One (1) New Hampshire resident was impacted by this incident. A notification letter was sent to the affected individual on February 2, 2018 via regular mail (a copy of the form notification letter is enclosed).

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

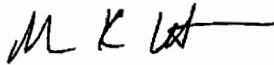
DCFG took immediate action to address this incident and prevent a similar incident in the future. Passwords to all employee e-mail accounts were changed, additional e-mail security enhancements were implemented, and additional training was provided to employees on recognizing and appropriately responding to suspicious emails and other security threats. Additionally, affected individuals were offered credit monitoring and identity restoration services free of charge for one year through AllClear ID.

4. Contact information.

DCFG remains dedicated to protecting the confidential information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at MVentrone@ThompsonCoburn.com or (312) 580-2219.

Very truly yours,

Thompson Coburn LLP

A handwritten signature in black ink, appearing to read "M K Ventrone", with a horizontal line extending to the right.

Melissa K. Ventrone

Enclosure

DATE

NAME

ADDRESS

CITY STATE ZIP

Notice of Data Security Incident

Dear NAME:

We are writing this letter to notify you of a recent data security incident experienced by DiFilippo Corporate Finance Group, Inc. ("DCFG") that may have impacted your personal information, including your name and Social Security number. We value and respect the privacy of your information, and 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 resources we are making available to help you.

What happened:

On December 14, 2017, we discovered suspicious activity involving an employee's email account. We took immediate steps to secure the account and hired an independent computer forensic firm to assist with investigating this matter. On January 12, 2018, the forensic investigation determined that an unauthorized user gained access to the email account through a phishing attack and may have been able to open and download emails between December 5 and December 14, 2017. We conducted a detailed review of the impacted account and determined your name and Social Security number were contained in an email attachment. Although we have no evidence that your information was actually viewed by the unauthorized user, we wanted to inform you of this incident out of an abundance of caution.

What we are doing and what you can do:

Although we do not believe the unauthorized user was interested in your personal information, we have arranged for you to receive credit monitoring and identity protection services from AllClearID, which we are offering at no cost to you for two years. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: 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 help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: XXXXXXXX.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

We also want you to know that we took immediate action to address this incident and prevent a similar incident in the future. Passwords to all employee e-mail accounts were changed, we implemented additional e-mail security enhancements, and also provided additional training to our employees on recognizing and appropriately responding to suspicious emails and other security threats.

For more information:

If you have any questions or concerns, please call me directly at 1-978-462-2266, Monday through Friday, 9am-5pm EST. Your trust is a top priority for DCFG, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Paul DiFilippo
President and Managing Director
DiFilippo Corporate Finance Group, Inc.

U.S. State Notification Requirements

Fraud Alerts: You can place fraud alerts with the three credit bureaus 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 credit bureaus is below.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to send a request to each consumer reporting agency by certified mail, overnight mail, or regular stamped mail. 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, but is 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 agencies:

Equifax Security Freeze

P.O. Box 105069
Atlanta, GA 30348
www.equifax.com

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
<http://www.experian.com/freeze>

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
www.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed below:

Federal Trade Commission

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

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:

- 12 months of coverage 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 for 12 months from the date of the breach incident notification you received from Company (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:

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