Morgan Lewis

STATE OF NH
DEPT OF JUSTICE
2017 FEB 23 AM 10: 16

Ezra D. Church
Partner
215.963.5710
Ezra.church@morganlewis.com

VIA OVERNIGHT MAIL

February 22, 2017

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

Re: *Notification of Potential Security Breach*

Dear Office of the Attorney General:

This Firm represents Fresh Formats LLC ("Fresh Formats") in connection with a situation where malware was detected on the computer of a Fresh Formats Human Resources employee. This employee had a file on her computer containing personal information of Fresh Formats associates. It is unclear if the malware detected on the computer actually was used to obtain any personal information from the file. Upon learning of the incident, Fresh Formats removed the malware from the computer and is taking steps to be sure an incident like this does not occur again.

At this time, we have not received any reports of improper use of the affected individuals' personal information. Nonetheless, Fresh Formats is sending notification letters out to all individuals whose personal information was contained in the computer file. In addition, Fresh Formats is offering a two-year subscription to All Clear ID's Identity Repair and Credit Monitoring Services.

Further information about what Fresh Formats has done and what we are recommending to the individuals in question can be found in the enclosed notification letter that Fresh Formats sent to one New Hampshire resident.

If you have any questions, please feel free to contact me.

Regards,

Ezra D. Church

Enclosures

Morgan, Lewis & Bockius LLP

1701 Market Street
Philadelphia, PA 19103-2921
United States

T +1.215.963.5000
F +1.215.963.5001

fresh FORMATS

[Name]
[Address]

Re: Notice of Potential Unauthorized Access to Personal Information

Dear [First Name]:

We are writing to tell you about a data security incident that may have exposed some of your personal information. While we have no reason to believe that this information has been or will be used inappropriately, we would like to let you know what happened, what information was involved, what we have done to address the situation, and to remind you of what you can do to protect your continued privacy.

What Happened?

On or about November 10, 2016, our Information Technology Department detected malware on a Fresh Formats HR associate's computer. This associate had a file on her computer containing personal information of Fresh Formats associates. It is unclear if the malware detected on the computer actually was used to obtain any personal information from the file.

What Information Was Involved

The file contained the names, addresses and Social Security numbers of Fresh Formats associates. To date, we have not received any reports of improper use of any of this information.

What We Are Doing

Fresh Formats takes these types of situations very seriously. Since we learned this information, we have launched an investigation to determine how the malware got onto the HR associate's computer and how we can prevent this from occurring again in the future.

What You Can Do

There are several steps you can take to protect your continued privacy and be sure that the information is not used improperly, many of which are good practices in any event.

First, as an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months:

- *AllClear Identity Repair:* This service is automatically available to you with no enrollment required. If a problem arises, simply call 855-270-9182 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 or by phone by calling 855-270-9182 using the following redemption code: {RedemptionCode}.

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

Second, contact any financial institutions that you bank with and advise them of this situation, particularly if any of them use your social security number to identify or verify you. Check your accounts online or via telephone for any potential fraudulent activity. You should check your periodic statements from each such financial institution or credit card company promptly upon receiving them to be sure that no unauthorized transactions have occurred.

For More Information

For general information on protecting your privacy and preventing unauthorized use of your personal information, you may visit the U.S. Federal Trade Commission's Web site, http://ftc.gov or contact your state office of consumer affairs or attorney general. You can also see the attached "Reference Guide" for more information relevant to your state.

* * *

We are committed to maintaining the security and privacy of the personal information you entrusted to us. We apologize for any inconvenience or concern this incident may cause. If we can be of any further assistance or answer any questions, or you encounter any problems that you believe to be related to this incident please call Anna Lehman at 717-240-5502.

Sincerely,

Michelle Castellana

Michelle Castellana

Reference Guide

In the event that you ever suspect that you are a victim of identity theft, we encourage you to consider taking the following steps:

Contact the Federal Trade Commission. You can contact the Federal Trade Commission's Consumer Response Center at 600 Pennsylvania Avenue, NW, Washington, DC, 20580 or 1-877-IDTHEFT (438-4338) or at http://www.ftc.gov/bcp/menus/business/data.shtm, to obtain more information about steps you can take to avoid identity theft. If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

Place a Fraud Alert on Your Credit File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You may wish to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze by contacting the credit bureaus at:

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, California 92834-6790	800-680-7289	www.transunion.com

The credit bureaus may charge a reasonable fee to place a freeze on your account, and may require that you provide proper identification prior to honoring your request. 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 the police report, investigative report, or complaint to law enforcement agency concerning identity theft
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.

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at:

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

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. 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 $5 each to place, temporarily lift, or permanently remove a security freeze.