

January 7, 2022

Anjali C Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via E-mail: IDTheft@oaq.state.md.us

Attorney General Brian Frosh

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Cybersecurity Incident
Client: New York Flower, LLC.
File No.: 15991.01071

Dear Attorney General Frosh:

We represent New York Flower, LLC. ("NYF") a real estate management firm operating in New York City, New York in regards to a recent cybersecurity incident. NYF takes this matter very seriously and is taking measures to remediate the incident and provide notice to potentially affected individuals.

This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of Maryland residents being notified, and the steps that NYF has taken in response to the incident.

1. Nature of the incident.

On or about July 7, 2021, NYF became aware of a potential business email compromise event after being notified of an outgoing spam campaign that originated from an NYF employee account. NYF immediately contacted their IT support team, who began an investigation into the incident. As a result of the preliminary investigation, NYF contacted third party cybersecurity experts to conduct a thorough investigation to determine the nature and scope of the incident. Based on the results of the investigation, it was determined that an unauthorized party may have been able to access sensitive personal information for some of our clients.

NYF subsequently launched a second investigation to determine which individuals may have been impacted. This investigation concluded with the production of a list of individuals. Based on this list, NYF engaged in a substantial data validation process to verify the accuracy of the data. Immediately after concluding its validation procedures, NYF procured credit monitoring for affected individuals and drafted notices to individuals and state and federal regulators as appropriate.

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

The forensics investigation revealed that those who instigated the cybersecurity attack gained access to emails containing personal information. PII impacted includes individual names in combination with one or more of the following: social security number, driver's license number, and/or financial account information.

2. Number of Maryland residents affected.

NYF discovered that three (3) residents of Maryland were impacted by this incident. A notification letter was sent to the individuals on January 10, 2022. A sample notice letter that was sent to the impacted individuals is included as **Exhibit A**.

3. Steps taken.

NYF is committed to taking action as needed to address the situation and to help ensure that a similar situation does not occur in the future by adding the following security controls: Implemented new email settings and security procedures and updated the password policy for all employees.

NYF has also provided 12 months of credit monitoring to the individuals whose PII was potentially accessed by an unauthorized individual.

4. Contact information.

NYF remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP



Anjali C. Das

Enclosure

EXHIBIT A

New York Flower LLC
P.O. Box 3923
Syracuse, NY 13220

NEW YORK FLOWER LLC
489 FIFTH AVENUE, 6TH FLOOR
NEW YORK, NY 10017
212-371-5050

<Individual Name>
<Address 1>
<Address 2>

Notice of Cybersecurity Incident

January 10, 2022

Dear <Individual Name>,

We are writing to inform you of a cybersecurity incident which affected New York Flower, LLC (“NYF”). The cybersecurity incident may have resulted in the potential compromise of some of your personal information. This letter contains information about the incident and information about how to protect your personal information going forward. NYF considers the protection of sensitive information a top priority, and sincerely apologizes for any inconvenience as a result of the incident.

Who We Are and Why We Have Your Data

NYF is an organization that consists of multiple, affiliated real estate firms and provides administrative and organizational support to those firms. It is possible NYF was in possession of your personal information as a result of this relationship.

What Happened

On or about July 7, 2021, NYF became aware of a potential business email compromise event after being notified of an outgoing spam campaign that originated from an NYF employee account. NYF immediately contacted their IT support team, who began an investigation into the incident. As a result of the preliminary investigation, NYF contacted third party cybersecurity experts to conduct a thorough investigation to determine the nature and scope of the incident. Based on the results of the investigation, it was determined that an unauthorized party may have been able to access sensitive personal information for some of our clients.

NYF subsequently launched a second investigation to determine which individuals may have been impacted. This investigation concluded with the production of a list of individuals. Based on this list, NYF engaged in a substantial data validation process to verify the accuracy of the data. Immediately after concluding its validation procedures, NYF procured credit monitoring for affected individuals and drafted notices to individuals and state and federal regulators as appropriate.

What Information Was Involved

While we have no reason to believe that your information has been misused as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the

* Services marked with an “*” require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

investigation, the unauthorized party may have had access to one or more of the following information: name, social security number, driver's license number, and/or financial account information. Please note that not every data element was present for every individual. While we appreciate that the incident may be concerning, please note that NYF has no evidence of misuse of sensitive information.

What We Are Doing

NYF engaged a specialized cybersecurity firm to conduct an investigation of the incident. Since the incident, NYF has continued to strengthen their security posture by adding the following security controls: Implemented new email settings and security procedures and updated the password policy for all employees.

Additionally, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring* services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: <Code>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What You Can Do

We recommend that you continue to remain vigilant in monitoring your personal information. The easiest way to do this is to take advantage of the complimentary credit monitoring and identity theft services we are offering to you. Details regarding these services are included in a separate attachment to this letter.

There are additional steps you can take to protect yourself which are contained in the supplement to this letter titled "*Additional Important Information.*"

The protection of your information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause. If you have any questions, please do not hesitate to call 1-800-405-6108 Monday through Friday, between 8:00 am to 8:00 pm Eastern time.

Sincerely,

New York Flower, LLC.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law 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.

For residents of Illinois, Iowa, Maryland, 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. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

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, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov

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

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

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 all states:

Fair Credit Reporting Act: You are also advised that you may have additional rights under the federal Fair Credit Reporting Act.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for

* Services marked with an “*” require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

all three credit bureaus are at the bottom of this page.

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 make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

[\(800\)-525-6285](tel:(800)525-6285)

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

[\(888\)-397-3742](tel:(888)397-3742)

www.experian.com/freeze

TransUnion (FVAD)

P.O. Box 2000

Chester, PA 19022

[\(800\)-680-7289](tel:(800)680-7289)

freeze.transunion.com

More information can also be obtained by contacting the Federal Trade Commission listed above.

* Services marked with an “*” require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.