MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

May 21, 2021

**VIA U.S. MAIL**

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

**Re: *Notice of Data Event***

Dear Sir or Madam:

We represent the City of Avon Park, Florida ("Avon Park") located at 110 E Main Street, Avon Park, Florida 33825, and are writing to notify your Office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Avon Park does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On December 9, 2020, Avon Park learned that it was the target of a cybercriminal attack and that portions of its computer network were infected with malware. Avon Park immediately took systems offline and launched an investigation into the nature and scope of the incident. On or about January 15, 2021, the investigation determined that certain files stored within Avon Park's network may have been available to the unauthorized actor. Following a thorough and time-consuming review of the systems in question, which was completed on March 28, 2021, Avon Park determined that certain files stored within the affected systems contained individuals' name, bank account information, driver's license number, and/or Social Security number.

**Notice to New Hampshire Residents**

On or about May 21, 2021 Avon Park provided written notice of this incident to affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

**Other Steps Taken and To Be Taken**

Upon discovering the event, Avon Park moved quickly to investigate and respond to the incident, assess the security of Avon Park's systems, and notify potentially affected individuals. Avon Park is also working to implement additional safeguards and training to its employees and is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

Additionally, Avon Park is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

GCL:rrg
Enclosure

# Exhibit A

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

**Notice of Data Breach**

Dear <<Name 1>>:

The City of Avon Park, Florida (the "City") is writing to make you aware of an incident that may impact some of your information. While we are unaware of any actual or attempted misuse of your information, we write to provide you with information about the event, our response, and steps you may take to better protect your information, should you feel it is appropriate to do so.

***What Happened?*** On December 9, 2020, the City learned that it was the target of a cybercriminal attack and that portions of our computer network were infected with malware. We immediately took systems offline and launched an investigation into the nature and scope of the incident. On or about January 15, 2021, our investigation determined that certain files stored within the City's network may have been available to the unauthorized actor. Following a thorough and time-consuming review of the systems in question, which was completed on March 28, 2021, the City determined that certain files stored within the affected systems that contain your information could have been accessed by the cybercriminal. Although at this time there is no indication that your information was accessed or misused, the City is providing notice to you in an abundance of caution because the affected systems contained certain information related to you.

***What Information was Involved?*** Our investigation determined that the information present may include a combination of your name <<Breached Elements>>.

***What we are Doing.*** Upon learning of this incident, the City took steps to secure our systems and began a review to determine what information may be at risk. We are also reviewing existing security policies and procedures and have implemented additional measures to further protect against similar incidents in the future. This incident has been reported to law enforcement and applicable state regulators.

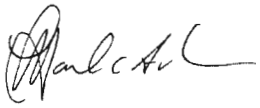
As an added precaution, we are offering you access to credit monitoring and identity theft protection services for **<<CM Length>>** months at no cost to you. You will find information on how to enroll in these services in the enclosed "*Steps You Can Take to Help Protect Your Information.*" We encourage you to enroll in these services as we are not able to do so on your behalf.

***What You Can Do.*** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Information.*"

***For More Information.*** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-654-0830 which is available Monday through Friday from 9:00 am to 9:00 pm Eastern Time.

We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Mark C. Schrader
City Manager
The City of Avon Park, Florida

## *Steps You Can Take to Help Protect Your Information*

### Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online **credit monitoring service** (*my*TrueIdentity) provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

**How to Enroll: You can sign up online or via U.S. mail delivery.**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based, three-bureau credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static 6-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

**ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and credit score.
- The daily three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

### Monitor Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

| Equifax | Experian | TransUnion |
|---|---|---|
| https://www.equifax.com/personal/credit-report-services/ | https://www.experian.com/help/ | https://www.transunion.com/credit-help |
| 888-298-0045 | 1-888-397-3742 | 833-395-6938 |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069 | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013 | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016 |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788 | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013 | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094 |

**Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**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. **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, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **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.