



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 08 2020

CONSUMER PROTECTION

Jim E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 1, 2020

VIA U.S. MAIL

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

Re: Notice of Data Security Incident

Dear Sir or Madam:

We represent The City of Fort Lauderdale (“Fort Lauderdale”) headquartered at 100 N. Andrews Ave, 2nd Floor, Fort Lauderdale, FL 33301, and are writing to provide notice to your office of an incident that may affect the security of personal information relating to certain New Hampshire residents. This notice may be supplemented if significant facts are learned subsequent to its submission. By providing this notice, Fort Lauderdale does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

Nature of the Data Event

On March 20, 2020, The City was notified by its vendor, Paperless Pay, of a data security event that had occurred on February 19, 2020. Paperless was informed by the Department of Homeland Security that an unknown individual had advertised the sale of access to its database on the dark web. Paperless launched an investigation and confirmed that an unknown actor had gained access to its database. On April 4, 2020, Fort Lauderdale confirmed that the database contained names and Social Security numbers for certain Fort Lauderdale former and current employees. Fort Lauderdale provided notice to individuals of the event, and arranged for credit monitoring to be provided to all impacted individuals.

Notice to New Hampshire Residents

On or about May 1, 2020, Fort Lauderdale provided written notice of this incident to all affected individuals, which includes twelve (12) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Fort Lauderdale moved quickly to investigate the incident, minimize risk to the information, and to provide the affected individuals with notice of this incident. Fort Lauderdale is working to implement additional safeguards and training to its employees.

Additionally, Fort Lauderdale is providing all impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to law enforcement. Fort Lauderdale is also providing individuals with complimentary credit monitoring, and information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. Fort Lauderdale is also providing written notice of this incident to other state regulators, as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,



Jim E. Prendergast of
MULLEN COUGHLIN LLC

ENCLOSURE
JEP:HFH

EXHIBIT A



CITY OF
FORT LAUDERDALE

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

May 1, 2020

F4933-L01-0000001 P001 T00001 *****ALL FOR AADC 159



SAMPLE A SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



Re: Notice of Data Event

Sample A Sample:

The City of Fort Lauderdale (“The City”) is writing to advise you of the potential unauthorized access to your personal information held by the City’s payroll and tax document printing vendor, PaperlessPay Corporation (“Paperless”). We write to provide you with information about the event, steps taken since discovering the event, and what you can do to better protect against potential misuse of your information as a result of this event, should you feel it is appropriate to do so.

What Happened? On March 20, 2020, The City was notified by Paperless of a data security event that had occurred on February 19, 2020. Paperless was informed by the Department of Homeland Security that an unknown individual had advertised the sale of access to its database on the dark web. Paperless launched an investigation and confirmed that an unknown actor had gained access to its database.

What Information was Affected? The database contained the following of your personal information: your name, address while working for the City of Fort Lauderdale, and your Social Security number.

What Are We Doing? The City takes the security of personal information very seriously. Upon learning of this event on March 20, 2020, The City immediately launched an investigation to determine the nature of this incident. In addition to providing notice of this event to you, The City will be providing notice to relevant state regulators.

What Can You Do? The City encourages you to review your accounts for suspicious activity, and immediately report all suspicious activity to the institution that issued the record. To the extent it is helpful, we are offering additional steps you can take to protect your information on the following pages. We are also extending an offer of ## months of credit monitoring through Experian.

For More Information: The City understands you may have questions that are not addressed in this letter. Should you have any questions or concerns regarding this incident, please call our dedicated toll-free line at **(844) 439-7669, Monday through Friday, 9:00 a.m. to 9:00 p.m ET, Saturday through Sunday 11:00 a.m. to 8:00 p.m. ET.** This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information.

0000001



F4933-L01

We sincerely regret the inconvenience this incident with the vendor's database may cause you. The City remains committed to safeguarding the information in its care and will continue to take steps to ensure the security of your data.

Sincerely,

A handwritten signature in black ink, appearing to read "Tarlesha W. Smith". The signature is written in a cursive style with a prominent initial "T".

Tarlesha W. Smith
Assistant City Manager/ Director of Human Resources

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary ###-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: July 31, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 439-7669 by **July 31, 2020**. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your ##-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (844) 439-7669. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*



Monitor Your Accounts

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

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

PO Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

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 a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.

For Maryland Residents: the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina Residents: the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two Rhode Island residents impacted by this incident.

For New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

000001



F4933-L01