

# **EXHIBIT 1**

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, the City of Jacksonville Beach, FL (“COJB”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.<sup>1</sup>

### **Nature of the Data Event**

On or about January 29, 2024, COJB began experiencing information system issues as a result of a cybersecurity event. In response, COJB immediately took steps to secure its computer systems and launched an investigation with the assistance of third-party specialists. This investigation determined that certain files in COJB systems were subject to unauthorized access and that information may have been taken from the network between January 22, 2024 through January 29, 2024. As a result, COJB began a thorough review of the data stored within these files to determine the type of information was contained within them and to whom the information relates. On or about February 22, 2024, this review determined that sensitive information pertaining to certain individuals was potentially involved in this incident and includes names and Social Security numbers.

### **Notice to Maine Residents**

On or about March 20, 2024, COJB will be providing written notice of this incident to approximately thirty-eight (38) Maine 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, COJB moved quickly to investigate and respond to the incident, assess the security of COJB systems, and identify potentially affected individuals. Further, COJB notified federal law enforcement regarding the event. COJB is also working to implement additional safeguards and training to its employees. COJB is providing access to complimentary credit monitoring services for twelve (12) months, through Epiq, to individuals whose information was potentially affected by this incident.

Additionally, COJB 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.

COJB is providing written notice of this incident to relevant state regulators and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

---

<sup>1</sup> COJB is a political subdivision of the State of Florida and shares state sovereignty and therefore is not subject to the laws of other states.

# **EXHIBIT A**



Secure Processing Center  
25 Route 111, P.O. Box 1048  
Smithtown, NY 11787

<<Name 1>> <<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>

<<Date>>

**NOTICE OF <<VARIABLE HEADER/ Data 1>>**

Dear <<Name 1>> <<Name 2>>:

The City of Jacksonville Beach, FL (“COJB”) is writing to notify you of a recent incident that may impact the privacy of some of your information. This letter provides you with information about the incident, our response, and steps you may take to protect your information, should you find it necessary to do so.

**What Happened?** On or about January 29, 2024, COJB began experiencing information system issues as a result of a cybersecurity event. We immediately took steps to secure our systems and launched an investigation. This investigation determined that certain files in our systems were subject to unauthorized access and that information may have been taken from our network between January 22, 2024 through January 29, 2024.

**What Information Was Involved?** As a result, we began a thorough review of the data stored within these files to determine the type of information contained within them and to whom the information relates. This review recently determined these files include sensitive information for certain individuals, including you. We are notifying you now because the information potentially involved in this event includes your <<Breached elements>> and name.

**What We Are Doing.** The confidentiality, privacy, and security of information within our care is among our highest priorities. Upon learning of the event, we have taken additional steps to implement enhanced security measures and better protect against similar incidents in the future. We are also notifying applicable regulators of the event.

Additionally, we are offering complimentary credit monitoring and identity theft protection services for <<CM Duration>> months through Equifax. Please note that you will not be automatically enrolled in these services as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the *Steps You Can Take to Help Protect Your Information* section below.

**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. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity theft protection services we are making available to you.

**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 844-709-0703, between the hours of 9:00 AM –9:00 PM Eastern Time, Monday through Friday, excluding major U.S. holidays. You can also write to COJB at 11 North Third Street, Jacksonville Beach, FL 32250.

We sincerely regret any inconvenience this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

*City of Jacksonville Beach, FL*

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### **Enroll in Credit Monitoring and Restoration**

**Activation Code:** <ACTIVATION CODE>

**Enrollment Deadline:** <DEADLINE MMMM DD, YYYY>

### **Equifax Credit Watch™ Gold**

\*Note: You must be over age 18 with a credit file to take advantage of the product

#### **Key Features**

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications<sup>1</sup> when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft<sup>4</sup>

#### **Enrollment Instructions**

Go to [www.equifax.com/activate](http://www.equifax.com/activate)

Enter your unique Activation Code of <ACTIVATION CODE> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

*If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.*

*Once you have successfully signed in, you will skip to the Checkout Page in Step 4*

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

#### **You’re done!**

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

<sup>1</sup>WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded. <sup>2</sup>The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. <sup>3</sup>Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com) <sup>4</sup>The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. 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, 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 a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-

free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-800-916-8800
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**

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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.

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

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately [X] Rhode Island residents that may be impacted by this event.