

# **Exhibit 1**

By providing this notice, the Town of Concord 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.

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

On or about October 17, 2019, the Town of Concord underwent a routine replacement of a large amount of office equipment. Part of this process included disposing of hard drives used to store data related to Town business. These hard drives were delivered to Concord Public Works for disposal and were discovered missing just before the scheduled disposal. The Town of Concord Police Department immediately commenced a criminal investigation and, at this time, has not been able to recover the missing hard drives.

On November 14, 2019, the Town of Concord notified current employees of this incident by email, posted about this incident on the Town Facebook page, and posted a press release about this incident on the Town website. The Town of Concord also commenced an extensive review of existing systems to determine whose information could potentially be stored on the missing hard drives. Out of an abundance of caution, the Town of Concord decided to provide identity protection services to current employees, retirees, and dependents even though the Town of Concord is not aware of any misuse of anyone's information in connection with this incident.

The information that could have been subject to unauthorized access includes name, address, and Social Security number.

### **Notice to Maine Residents**

Following the extensive review of data, on or about September 15, 2020, the Town of Concord began providing written notice of this incident to affected individuals, which includes thirteen (13) 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, the Town of Concord moved quickly to investigate and respond to the incident, reset old passwords, change access procedures, and notify potentially affected individuals. The Town of Concord is also reviewing its existing policies and procedures and implanting additional safeguards to enhance the security of information in its possession. The Town of Concord is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, the Town of Concord is providing 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 their credit card company and/or bank. The Town of Concord is providing individuals with 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.

# **Exhibit A**



TOWN OF CONCORD

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<MemberFirstName>> <<MemberLastName>>,

The Town of Concord writes to you regarding an incident that may affect the security of some of your personal information. This letter contains information about the incident, our response, and steps you may take to better protect your personal information, should you feel it necessary to do so.

**What Happened?** On October 17, 2019, the Town of Concord underwent a routine replacement of a large amount of office equipment. Part of this process included disposing of hard drives used to store data related to Town business. These hard drives were delivered to Concord Public Works for disposal and were discovered missing just before the scheduled disposal. The Town of Concord Police Department immediately commenced a criminal investigation and, at this time, has not been able to recover the missing hard drives.

On November 14, 2019, we notified current employees of this incident by email, posted about this incident on the Town Facebook page, and posted a press release about this incident on the Town website. We also commenced an extensive review of existing systems to determine whose information could potentially be stored on the missing hard drives. Out of an abundance of caution, we decided to provide identity protection services to current employees, retirees, and dependents even though we are not aware of any misuse of anyone's information.

**What Information Was Involved?** The Town of Concord engaged outside forensic experts to work with our team to understand what information was stored on the missing hard drives. We determined that your name and Social Security number may have been stored on the missing hard drives.

**What Are We Doing?** We take this matter and the security of your personal information very seriously. Out of an abundance of caution, we have reset old passwords and changed access procedures. As part of our ongoing commitment to the security of personal information in our care, we are also reviewing our existing policies and procedures and implementing additional safeguards to enhance the security of information in our possession.

As an added precaution, we are also offering you complimentary access to 12 months of identity monitoring and restoration services through Kroll. We encourage you to activate in these services, as we are not able to act on your behalf to activate you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

**What Can You Do?** We encourage you to review the enclosed *Steps You Can Take To Help Protect Your Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also enroll to receive the free credit and identity monitoring services we are offering.

**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 1-844-915-2896 Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time.

We sincerely regret any concern this incident may cause you. Protecting your information is a top priority for the Town of Concord and we remain committed to safeguarding your personal information.

Sincerely,

A handwritten signature in black ink, consisting of several overlapping loops and a long horizontal stroke at the bottom.

Stephen Crane  
Town Manager

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Enroll in Credit and Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **November 2, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

You've been provided with access to the following services<sup>1</sup> from Kroll:

**Single Bureau Credit Monitoring.** You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

**Fraud Consultation.** You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

**Identity Theft Restoration.** If you become a victim of identity theft, an experienced Kroll licensed investigation will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

### Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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**

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

#### **TransUnion**

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

#### **Equifax**

P.O. Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
- 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 9554  
 Allen, TX 75013  
 1-888-397-3742  
[www.experian.com/fraud/center.html](http://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](http://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](http://www.equifax.com/personal/credit-report-services)

**Additional Information**

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](http://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.

**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](http://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](http://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](http://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. <<b2b\_text\_1(RIStatement)>>.

**For Washington, D.C. residents**, the Office of Attorney General for the District of Columbia can be reached at: 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.