

# EXHIBIT 1

By providing this notice, Monroe, Sweeris & Tromp PLC (“MS&T”) MS&T 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 May 14, 2020, MS&T discovered suspicious activity in an MS&T office administrator’s email account. Upon learning of this activity, MS&T immediately took steps to secure the email account and began an investigation to determine the nature and scope of the activity. The investigation determined that an unknown actor gained unauthorized access to the MS&T employee’s email account on one known occasion between May 11, 2020 and May 14, 2020. During this limited timeframe, the unauthorized actor could have had access to certain emails and attachments within the account. MS&T’s investigation, with the assistance of third-party information technology consultants, determined that only one MS&T email account was impacted and that there was no evidence of access to internal MS&T systems or that the contents of the email account was downloaded by the unknown actor. While the investigation was able to identify evidence that one email within the account was accessed by the unknown actor, in an abundance of caution, MS&T conducted a review of the entire account.

On July 16, 2020, with the assistance of third-party forensics, MS&T completed the review of the contents of the email account to determine the types of protected information contained in the emails and to whom the information relates, and immediately launched a review of its files to ascertain address information for the impacted individuals. This review determined that the following types of information was present within the account at the time of this incident: name, Social Security number, and personal tax identification number.

### **Notice to Maine Residents**

On or about October 5, 2020, MS&T began providing written notice of this incident to affected individuals, which includes two (2) 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, MS&T moved quickly to investigate and respond to the incident, assess the security of MS&T systems, and notify potentially affected individuals. MS&T is also reviewing existing policies and procedures and additional training to its employees. MS&T is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, MS&T is providing impacted individuals with guidance on how to better protect against identity theft and fraud, 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.

# EXHIBIT A



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

October 5, 2020

F8541-L01-0000001 T00001 P001 \*\*\*\*\*MIXED AADC 159



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



**Re: Notice of Data EXTRA1**

Dear Sample A Sample:

Monroe, Sweeris & Tromp PLC (“MS&T”) is writing to inform you of a recent matter that could possibly affect the security of some of your personal information. While **we are unaware of any actual or attempted misuse of your personal information**, we are providing you with information about the matter, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On May 14, 2020, MS&T discovered suspicious activity in a MS&T office administrator’s email account. Upon learning of this activity, MS&T immediately took steps to secure the email account and began an investigation to determine the nature and scope of the activity. The investigation determined that an unknown actor gained unauthorized access to the MS&T office administrator’s email account on one known occasion between May 11, 2020 and May 14, 2020. During this limited timeframe, the unauthorized actor could have had access to certain emails and attachments within the account. Our investigation, with the assistance of third-party information technology consultants, determined that only one MS&T email account was impacted and that there was no evidence of access to internal MS&T systems or that the contents of the email account was downloaded by the unknown actor. While the investigation was able to identify evidence that one email within the account was accessed by the unknown actor, in an abundance of caution, MS&T conducted a review of the entire account and is providing notice to you.

**What Information Was Involved?** On July 16, 2020, with the assistance of third-party forensics, MS&T completed the review of the contents of the email account to determine the types of protected information contained in the emails and to whom the information relates, and immediately launched a review of its files to ascertain address information for the impacted individuals. Our review confirmed that your Extra2 Item1, Item2, Item3, Item4, ETC was present in the email account at the time of this incident. **To date, MS&T has not received any reports of actual or attempted misuse of your information.**

0000001



**What We Are Doing.** The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. Out of an abundance of caution, MS&T engaged third-party information technology consultants and a notification vendor in order to inform you of this matter. When we discovered this incident, we immediately reset the account password, and with the assistance of third-party information technology services, took steps to determine what personal data was at risk. We also confirmed the security of all employee email accounts and related systems. As part of our ongoing commitment to the security of personal information in our care, we continue to review our existing policies and procedures, and are committed to continuous training for our employees on data privacy and security. We also will be notifying state regulators, as required.

As an added precaution, we are also offering you complimentary access to EXTRA3 months of credit and identity monitoring, fraud consultation, and identity theft restoration services through Experian. We encourage you to activate these services, as we are not able to activate them on your behalf. Please review the instructions contained in the attached Steps You Can Take to Help Protect Your Information for additional information on these services.

**What You Can Do.** You may review the enclosed *Steps You Can Take to Help Protect Your Information*, which contains 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 activate the complimentary credit and identity monitoring services we are offering.

**For More Information.** We understand that you may have questions about this matter that are not addressed in this letter. If you have additional questions, please call MS&T at our dedicated assistance line at **(877) 355-3282** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). You may also write to MS&T at 6617 Crossings Drive SE, #100, Grand Rapids, Michigan 49508.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,



Monroe, Sweeris & Tromp PLC

## *STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION*

### **Enroll in Credit and Identity Monitoring**

To help protect your identity, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for EXTRA3 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. 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 from the date of the incident (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).

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary EXTRA3 month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

Please note that Identity Restoration is available to you for EXTRA3 months 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](http://www.ExperianIDWorks.com/restoration).

- Ensure that you **enroll by December 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: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332** by **December 31, 2020**. Be prepared to provide engagement number ENGAGEMENT as proof of eligibility for the Identity Restoration services by Experian.

### **ADDITIONAL DETAILS REGARDING YOUR EXTRA4 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.\*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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

\*\*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.

0000001



## **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:

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 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. 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](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 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/>.

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

