

EXHIBIT 1

By providing this notice, Holthouse Carlin & Van Trigt LLP (“HCVT”) 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 October 14, 2020, HCVT became aware of suspicious activity related to an employee email account. HCVT immediately launched an investigation to determine the full nature of the scope of the event. The investigation determined that an unknown individual accessed the HCVT employee’s email account at various times between October 7, 2020 and October 14, 2020.

HCVT then undertook a comprehensive and time consuming programmatic and manual review of all potentially disclosed data. This extensive review process was undertaken to identify the type of information potentially impacted and to whom the information related. This impacted data related to individuals associated with HCVT’s business clients who are the Data Owners. On April 16, 2021, HCVT began notifying the impacted Data Owners of this event and provided information regarding the impacted individuals associated with the Data Owners. HCVT then obtained consent to notify individuals from the owners of the data on their behalf. Although HCVT is unaware of any actual misuse of data impacted by this event, they are notifying potentially affected individuals out of an abundance of caution.

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

Notice to Maine Resident

On or about June 18, 2021, HCVT began providing written notice of this incident to affected individuals, which includes one (1) Maine resident. 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, HCVT moved quickly to investigate and respond to the incident, assess the security of HCVT systems, and notify potentially affected individuals. HCVT is also working to implement additional safeguards and training to its employees. HCVT is providing access to credit monitoring services for one (1) year through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HCVT 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. HCVT is providing individuals with 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

June 18, 2021

G5405-L01-0000001 T00001 P001 *****AUTO**MIXED AADC 159



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



Re: Notice of Data Breach

Dear Sample A. Sample:

Holthouse Carlin & Van Trigt LLP (“HCVT”) provides tax, accounting, business management, and auditing services to businesses and individuals, including [EXTRA3] and writes to notify you of an incident that may affect the privacy of some of your information. HCVT takes the protection of your information very seriously, and although we have no evidence of actual or attempted misuse of your information relating to this incident, this letter provides details regarding the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On October 14, 2020, HCVT became aware of suspicious activity related to an employee email account. We immediately launched an investigation to determine the full nature of the scope of the event. Our investigation determined that an unknown individual accessed the employee’s email account at various times between October 7, 2020 and October 14, 2020. Although there is no evidence that information relating to you was actually viewed by an unauthorized actor, that type of activity cannot be ruled out with complete certainty.

HCVT then undertook a comprehensive and time consuming programmatic and manual review of all potentially disclosed data. This extensive review process was undertaken to identify the type of information potentially impacted and to whom the information related. On March 2, 2021, HCVT’s investigation confirmed that the potentially impacted data included certain information relating to you.

What Information Was Involved? Although we are unaware of any actual or attempted misuse of your information, we are providing you this notification out of an abundance of caution because certain information relating to you was potentially accessed during this event. The potentially impacted information relating to you includes your name and [EXTRA2].

What We Are Doing. The privacy and security of information are among one of our highest priorities and HCVT has strict security measures in place to protect information in our care. Upon discovering this incident, we immediately took steps to protect the privacy and security of client, business partner, and employee information. We also reviewed existing security policies and implemented additional measures and enhanced security tools to further protect information in our systems. We also implemented additional safeguards and are providing additional training to our employees on data privacy and security. We reported this incident to regulatory authorities, as required by law.

0000001



In addition to providing notice of this event to you, we are also providing identity theft and credit monitoring protection services for 12 months through Experian at no cost to you. Information and instructions on how to enroll in these complimentary services can be found in the “Steps You Can Take to Help Protect Your Information” attached to this letter.

What Can You Do. 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. You may review the information contained in the attached “Steps You Can Take to Help Protect Your Information.” You may also enroll to receive the identity protection services we are making available to you. There is no charge to you for the cost of this service; however, you will need to enroll yourself in this service.

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (833) 549-2140 (toll free), Monday through Friday from 9 a.m. to 11 p.m. Eastern, and Saturday and Sunday from 11 a.m. to 8 p.m. Eastern.

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

Sincerely,

A handwritten signature in cursive script that reads "Patty O'Connell".

Patty O'Connell
Chief Operating Officer
Holthouse Carlin & Van Trigt LLP

Steps You Can Take to Help Protect Your Information

To help protect your identity, we are offering a complimentary 12 month 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: September 30, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: ABCDEFGHI**

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 (833) 549-2140 by **September 30, 2021**. Be prepared to provide engagement number **B014538** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12 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.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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 Insurance^{**}:** 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 (833) 549-2140. 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.

* 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, Financial, and Medical Billing Statements

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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. N.W. Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Holthouse Carlin & Van Trigt is located at 11444 W Olympic Blvd , Floor 11, Los Angeles, CA 90064-1500.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 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 [#] Rhode Island residents impacted by this incident.

For 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 bureaus 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 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. We encourage you to 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.

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/>.

