

EXHIBIT 1

By providing this notice, RKL LLP (“RKL”) 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 September 29, 2020, RKL received an informal notification from a Pennsylvania fraud investigator indicating that the investigator was working on a special project related to potential fraudulent tax returns filed for RKL clients. RKL immediately commenced an investigation, working with computer forensic specialists, to determine the existence and scope of a potential data incident. On November 2, 2020, RKL confirmed that certain RKL clients’ information was accessed by unauthorized individual(s) on separate occasions between April 22, 2020 and October 6, 2020.

RKL’s investigation into the incident is ongoing. Specifically, RKL commenced an extensive review of all messages and files at risk as a result of this incident to determine the entire population of information potentially accessible and to whom the information related. While the extensive review continues, RKL is notifying those clients and their spouses and/or dependents it knows may be impacted. The information that may have been subject to unauthorized access includes name, address, date of birth, Social Security number, and could also include information such as financial account information, individual taxpayer identification number or other government-issued identification number, driver’s license or state identification number, IRS Identity Protection (IP) PIN number, and/or medical/health insurance information, if it was contained in RKL tax files.

Notice to Maine Residents

On or about December 15, 2020, RKL provided 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, RKL moved quickly to investigate and respond to the incident, assess the security of RKL systems, reset all passwords, and notify potentially affected individuals. RKL is coordinating with the Internal Revenue Service (IRS) and it notified the state taxing authorities and law enforcement. RKL 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, RKL 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. RKL 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. RKL is notifying other state regulators as necessary.

EXHIBIT A

December 15, 2020



G0569-L02-0000002 T00017 P003 *****ALL FOR AADC 123
SAMPLE A SAMPLE - L02 INDIVIDUAL NOTICE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



[EXTRA1]

Dear Sample A Sample:

RKL LLP (RKL) is contacting you today to notify you of an incident that could potentially affect certain personal information relating to you. We take the security of personal information in our care seriously and are providing you with this notice to make you aware of the incident, our investigation to date, the steps we are taking in response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened?

On September 29, 2020, we received an informal notification from a Pennsylvania fraud investigator indicating that the investigator was working on a special project related to potential fraudulent tax returns filed for our clients. We immediately commenced an investigation, working with computer forensic specialists, to determine the existence and scope of a potential data incident. On November 2, 2020, we confirmed that certain RKL clients' information was accessed by unauthorized individual(s) on separate occasions between April 22, 2020 and October 6, 2020.

Our investigation into the incident is ongoing. Specifically, we commenced an extensive review of all messages and files at risk as a result of this incident to determine the entire population of information potentially accessible and to whom the information related. While the extensive review continues, we are notifying those clients and their spouses and/or dependents we know may be impacted.

What Information Was Involved?

Based on our review to date, we believe that certain personal identifying information may have been accessed without authorization, including your name, address, date of birth, Social Security number, and could also include information such as your financial account information, individual taxpayer identification number or other government-issued identification number, driver's license or state identification number, IRS Identity Protection (IP) PIN number, and/or medical/health insurance information, if it was in our tax files.

What We Are Doing?

We take this incident and the security of personal information entrusted to us very seriously. Upon initial discovery, we immediately commenced an investigation that included working with computer forensic specialists and coordinating with the IRS. We thereafter notified the state taxing authorities. We are providing you with the attached *Steps You Can Take to Protect Personal Information* that includes resources you may take advantage of to protect against potential fraud or misuse of your information.

0000002



RKL has secured the services of Experian to provide you with credit monitoring and identity restoration services for [XX] months, at no cost to you. More information on how to enroll in these services can be found in the enclosed Steps You Can Take to Protect Personal Information.

Information privacy and security are among our highest priorities. RKL has security measures in place to protect information in our care. Upon learning of this incident, RKL took steps to strengthen the security of our systems, including a reset of all passwords.

What You Can Do.

RKL encourages you to remain vigilant against incidents of potential fraud and/or misuse of your information, to review the enclosed *Steps You Can Take to Protect Personal Information*, and to enroll in the credit monitoring and identity restoration services we are offering.

For More Information. If you have questions about the services we are offering, suspicious activity, or the additional steps you can take to protect your information, we encourage you to call our dedicated assistance line at (888) 994-0272, available Monday through Friday, from 9:00 a.m. to 11:00 p.m., Eastern Time and Saturday/Sunday, from 11:00 a.m. to 8:00 p.m., Eastern Time.

We sincerely regret any inconvenience this incident may cause you. RKL takes the protection of the personal information within its care seriously and remains committed to safeguarding your information.

Sincerely,

A handwritten signature in black ink, appearing to read 'E. Monborne', with a long horizontal flourish extending to the right.

Edward W. Monborne
CEO, RKL LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in the Complimentary Credit Monitoring Services

To help protect your identity, we are offering a complimentary membership of Experian's® IdentityWorksSM for [XX] months. 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: 03/31/2021** (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 or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 994-0272 by **March 31, 2021**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

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 agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** 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 (888) 994-0272. 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).

Monitor Accounts Statements

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and credit reports for suspicious charges or claims. 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.

* 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.

0000002



G0569-L02

Place a Security Freeze

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

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

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

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, 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, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Request Fraud Alerts

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 one-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

TransUnion

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

www.transunion.com/fraud-alerts

Equifax

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

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; 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 District of Columbia residents, The Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-528-8663; and <https://www.marylandattorneygeneral.gov/>.

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 agencies 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 a 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 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; and www.ncdoj.gov.

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; 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 two Rhode Island residents impacted by this incident.

