CAMERON G. SHILLING
Direct Dial: 603.628.1351
Email: cameron.shilling@mclane.com
Admitted in NH and MA
900 Elm Street, P.O. Box 326
Manchester, NH 03105-0326
T 603.625.6464
F 603.625.5650

March 21, 2022

Via Email Only
Attorney General Austin Knudsen
Montana Department of Justice
215 N Sanders St.
Helena, MT 59601
ocpdatabreach@mt.gov

Re: Data Security Incident

To whom it may concern,

McLane Middleton, P.A. represents Roy & Rurak, which has its principal place of business at 158 Pleasant Street, North Andover, MA 01845. We are writing to inform you about a data security incident involving Roy & Rurak that affects 2 adults who are residents of Montana.

Please note that we are simultaneously providing you with notice on behalf of Paradis Raymond & Jalbert, which is an affiliate. Roy & Rurak and Paradis Raymond & Jalbert were both affected by this incident because they retain certain client-taxpayer information on a consolidated network.

What Happened: On December 29, 2021, Roy & Rurak discovered that a third party had obtained unauthorized remote access to Medaglia & Murphy's network. Medaglia & Murphy immediately contacted its managed information technology service provider (MSP), disabled the Internet connection to the network, and deactivated servers and computers on the network. The MSP removed all potential malware from the servers and computers, and rapidly rebuilt the network so the firms could continue to serve their clients during the tax preparation season.

At the same time that the MSP was performing that work, Roy & Rurak retained a cyber security attorney and a forensic expert to investigate and address this matter. The forensic expert first attempted to determine what information the third party had accessed. However, the forensics revealed only which portions of the network the third party accessed, not the particular information accessed.

As a result, Roy & Rurak initiated the process to notify the cyber security division of the Internal Revenue Service (IRS). Roy & Rurak did so immediately, even before it was able to identify or notify the population of affected individuals, in order to implement safeguards to mitigate the potential electronic filing of fraudulent tax returns, since the IRS electronic tax return filing system opened in mid-January 2022. Roy & Rurak supplied the IRS with the information necessary to activate the IRS's advance fraud detection and prevention system, called Return Integrity Compliance Services (RICS). Because Roy & Rurak timely initiated RICS, the IRS's accounts for all of its potentially affected clients and their dependents, including all individuals affected by the incident, have already had advance mechanisms implemented to detect and prevent the potential electronic filing of a fraudulent return for this tax year.

As Roy & Rurak was working with the IRS to initiate RICS, it received communications from the third party that accessed the network, confirming that they had done so and demanding a ransom in return for assurances about information they accessed. While Roy & Rurak did not need to pay ransom to restore its information and would not have considered doing so under other circumstances, it decided to engage with the third parties to assess their reliability and negotiate certain assurances from them. Roy & Rurak decided to do so because the firm wanted to provide its clients with as much assurance as possible concerning its efforts to protect their information.

To engage in these negotiations, Roy & Rurak communicated with and relied on federal law enforcement at the United States Secret Service (USSS), who have expertise with these situations. Based on the information Roy & Rurak learned during the negotiations, the USSS and its cyber security attorney and forensic expert felt that the third party actors were credible, and that Roy & Rurak could reasonably rely on their assurance that they would destroy the information they had accessed in return for the ransom payment. Thus, Roy & Rurak paid the ransom.

Before Roy & Rurak received the ransom demand, its forensic expert had been monitoring the dark web to detect if any information that might have been accessed on the network was being offered for sale on the dark web. Roy & Rurak's expert also has continued to do so after the ransom was paid. To date, Roy & Rurak has not discovered any such information on the dark web, and has no reason to believe that the third party actors released any information they accessed.

What Information Was Involved: Roy & Rurak's forensic expert was only able to determine which portions of Medaglia & Murphy's network the third party actors accessed, not what information may have been accessed. The portions of the network accessed by the third party contained the tax preparation files that Roy & Rurak maintains for its clients. Information in those tax preparation files varies from file-to-file. However, it commonly includes the following: social security numbers; financial account numbers; draft and completed tax returns; W-2, 1099, 1098, 1095, and other such income and tax forms; contact information; dates of birth; documents provided by clients to support their tax returns; and any other information Roy & Rurak may have received from clients.

What Was Done for Affected Individuals: Roy & Rurak retained Epiq to provide notification letters, call center services, and credit and identity monitoring and restoration protection to all individuals affected by the incident. The notices were mailed on March 16, 2022. Copies of the letters are attached. One letter is for adult taxpayers with at least one minor dependent, though such taxpayers may also have adult dependents. The second letter is for adult taxpayers with either no dependents or only adult dependents. The third is for adults whose information was in corporate tax returns. The duration of the protection services is two, and the services were offered to all affected adults and minors. Those services provide both credit and identity monitoring as well as dedicated fraud specialists to assist individuals restore their credit and identity in the event they experience any fraud.

Thank you for your attention to this matter. Please do not hesitate to contact us if you have any questions.

Very truly yours,

/s/ Cameron G. Shilling

Cameron G. Shilling

Enclosures

ROY & RURAK LLC

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Data Security Incident at Roy & Rurak

Dear Client,

We are writing to inform you about a data security incident experienced by Roy & Rurak that may have affected you and any of your dependents identified below in this letter. While Roy & Rurak's network was not compromised directly, Roy & Rurak uses the systems of an affiliate, Medaglia & Murphy, to retain certain information and prepare tax returns for certain clients, including you. You are receiving this letter because your information was in the portion of Medaglia & Murphy's system affected by the incident.

What Happened: On December 29, 2021, we discovered that a third party had obtained unauthorized remote access to Medaglia & Murphy's network. We immediately contacted Medaglia & Murphy's managed information technology service provider (MSP), disabled the Internet connection to the network, and deactivated servers and computers on the network. The MSP removed all potential malware from the servers and computers, and rapidly rebuilt the network so that we could continue to serve our clients during the tax preparation season.

At the same time that the MSP was performing that work, we retained a cyber security attorney and a forensic expert to investigate and address this matter. The forensic expert first attempted to determine what information the third party had accessed. However, the forensics revealed only which portions of the network the third party accessed, not the particular information accessed.

As a result, we initiated the process to notify the cyber security division of the Internal Revenue Service (IRS). We did so immediately, even before we were able to notify you, in order to implement safeguards to mitigate the potential electronic filing of fraudulent tax returns, since the IRS electronic tax return filing system opened in mid-January 2022. We supplied the IRS with the information necessary to activate the IRS's advance fraud detection and prevention system, called Return Integrity Compliance Services (RICS). Because we timely initiated RICS, the IRS's account for you has advance mechanisms implemented to detect and prevent the potential electronic filing of a fraudulent return for this tax year.

Because we initiated RICS, you may receive a communication from the IRS about that matter, including a request to submit certain tax forms to verify your identity, or to obtain an identity protection personal identification number (IP PIN) for the filing of electronic tax returns in the future. You may receive such a communication irrespective of whether or not a fraudulent tax return was filed in your name. If you receive such a communication, please contact us so we can assist you address that matter with the IRS.

As we were working with the IRS to activate RICS, Medaglia & Murphy received communications from the third party that accessed the network, confirming that they had done so and demanding a ransom in return for assurances about the information they accessed. While we did not need to pay ransom to restore the network and would not have considered doing so under other circumstances, we decided to engage with the third parties to assess their reliability and negotiate certain assurances from them. We decided to do so because we wanted to provide you and our other clients with as much assurance as possible concerning our efforts to protect your information.

To engage in these negotiations, we communicated with and relied on federal law enforcement specialists at the United States Secret Service (USSS), who have expertise with respect to these situations. Based on the information we learned during the negotiations, the USSS and our cyber security attorney and forensic expert felt that the third party actors were credible, and that we could reasonably rely on their assurance that they would destroy all of the information they had accessed in return for the ransom payment. We therefore paid the ransom.

Before we received the ransom demand, our forensic expert had already been monitoring a special part of the Internet used by these types of actors, called the dark web, to detect if any information that might have been accessed on our network was being offered for sale on the dark web. Our expert also has continued to do so after we paid the ransom. To date, we have not discovered any such information on the dark web. Thus, we have no reason to believe that the third party actors released any information they accessed.

What Information Was Involved: Our forensic expert was only able to determine which portions of the network the third party actors accessed, not what information may have been accessed. The portions of our network accessed by the third party contained the tax preparation files we maintain for our clients.

Information in our tax preparation files varies from file-to-file. However, it commonly includes the following: social security numbers; financial account numbers; draft and completed tax returns; W-2, 1099, 1098, 1095, and other such income and tax forms; contact information, including name, address, etc.; dates of birth; documents provided by clients to support their tax returns; and any other information we may have received from clients.

Our tax preparation files also commonly contain information about not only the taxpayer, but also the taxpayer's spouse and dependents. Our tax preparation file for you contained information about the following individuals.

<<TP First Last>>
<<SP First Last>>
<<AD1 First Last>>
<<AD2 First Last>>
<<AD3 First Last>>
<<AD4 First Last>>

What Should You Do: We initiated RICS to provide advanced fraud protection for your IRS account and mitigate the potential electronic filing of fraudulent tax returns this year. Thus, if you receive a communication from the IRS, such as a request to verify your identity or obtain an IP PIN, please contact us so that we can help you work with the IRS to address that matter.

Due to the significant volume of cyber security incidents this tax season, RICS is currently processing refunds only by check, not electronic deposit. While the IRS has informed us that RICS plans to return to electronic refunds, the IRS also could not provide us with any guarantee or timeline for doing so. As a result, if you are expecting an electronic refund, please look for a check instead. If you would like to monitor the status of your refund, you can do so at https://sa.www4.irs.gov/irfof/lang/en/irfofgetstatus.jsp. Please call us if you have any questions about that matter.

In addition to RICS, you should take another measure to protect yourself and the individuals listed above. In particular, we recommend enrollment in the credit and identity monitoring and restoration services described below. We are offering to pay for these protection services for you for 2 years. In light of the type of information involved in this incident, we feel that enrolling in these services is appropriate.

PLEASE BE AWARE THAT YOU HAVE UNTIL JUNE 30, 2022 TO ENROLL, SO PLEASE ENROLL PROMPTLY AND BY NO LATER THAN JUNE 30, 2022.

While we feel that RICS and the credit and identity protection services described below are sufficient, if you feel that additional measures are needed, some such steps are outlined in the "Steps You Can Take To Help Protect Your Information."

To enroll, please use the information and code below.

Enrollment Instructions

1. Go to https//www.equifax.com/activate
2. Enter the unique Activation Code associated with your name as follows.

<<TP First Last>>	<<TP Code>>
<<SP First Last>>	<<SP Code>>
<<AD1 First Last>>	<<AD1 Code>>
<<AD2 First Last>>	<<AD2 Code>>
<<AD3 First Last>>	<<AD3 Code>>
<<AD4 First Last>>	<<AD4 Code>>

Click "Submit" and complete the following 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.

Key Features

1. Credit monitoring with email notifications of key changes to your Equifax credit report
2. Daily access to your Equifax credit report
3. WebScan notifications when your personal information is found on fraudulent Internet trading sites
4. Automatic fraud alerts
5. Dedicated identity restoration specialist to help restore your identity should you be a victim of identity theft
6. Up to $1,000,000 of identity theft insurance for certain expenses resulting from identity theft

Police Report: We worked with the USSS to address this matter. Under certain state laws, you may have a right to obtain a copy of police reports. Also, if you feel that you have experienced identity or credit fraud or otherwise want to contact law enforcement about this matter, we encourage you to contact your federal, state or local law enforcement agency.

What Are We Doing: As noted above, we activated RICS, are notifying you about this incident and providing you with credit and identity monitoring and restoration services, and have worked with the MSP, cyber security attorneys and forensic expert to ensure that Medaglia & Murphy's network, servers, and computers are secure. While Medaglia & Murphy had meaningful cyber security safeguards in place before this incident occurred, even prepared businesses are not immune. As a result, we are working with the cyber security attorney and technology providers to conduct a comprehensive assessment of Medaglia & Murphy's technological, physical, and administrative processes in order to identify other potential opportunities to enhance our cyber security.

For More Information: If you have any questions about this incident, please contact us at response@medagliaco.com or (603) 816-2641. If you have any questions about the credit and identity monitoring and restoration services discussed below or need help enrolling in them, please contact Eqiq directly at 855-604-1877.

We value our relationship with you. Thus, we regret if this incident causes you concern, and are sincerely grateful for your continued support and trust in Roy & Rurak.

Sincerely,

Thomas A. Medaglia, Jr.

Steps You Can Take to Help Protect Your Information

Monitor Accounts

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.

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. 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 years, 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" 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 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-victim-resource/place-fraud-alert

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); 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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **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. You can 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. **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/. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident. **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. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.