

Rutherford, MacDonald & Olson, P.C.

Certified Public Accountants

Processing Center • P.O. BOX 141578 • Austin, TX 78714



00001
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

August 23, 2017

Private & Confidential

Dear John:

Re: **Notice of Data Breach**

We value the trust that you have placed in your relationship with Rutherford, MacDonald & Olson, P.C. We know that part of that trust is the expectation that the information that you provide to us will be secure and protected. We take our responsibility in that regard very seriously. That is why we are writing to you. We have discovered that, like many other businesses, government agencies, accounting firms, and tax preparers, we were a victim of unauthorized on-line access to our server.

What Happened? Based on the results of a forensic investigation we confirmed that someone was able to gain unauthorized access to our server in March and April of 2017.

What Information Was Involved? The unauthorized party was able to access our server, which contains, among other things, information relating to client tax returns — including Social Security Number, name, address, telephone number, and other state and federal income tax filing related information. While we do not have specific evidence that your information was fraudulently used, because that possibility exists we are providing you with information regarding this incident in an abundance of caution.

What We Are Doing: We notified all individuals affected, law enforcement, and the United States Internal Revenue Service about the security incident and the confidential data that may have been accessed. As an additional precaution we have engaged AllClear ID to protect your identity for 12 months at no cost to you.

What You Can Do: Please review the recommendations on the following page for steps you can take to protect your personal information and sign up for 12 months of complimentary identity protection services.

For More Information: If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident at 1-855-285-9868. The call center is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time (excluding U.S. holidays). If you require extra assistance, please contact Rutherford, MacDonald & Olson, P.C. by phone at (406) 926-1295 or by email at info@rmo-pc.com with the subject line "Data Breach."

Sincerely,

Rutherford, MacDonald & Olson P.C.

Rutherford, MacDonald & Olson P.C.



01-02-1-00

Important Information: Recommendations You Can Take to Protect Your Identity

Contact AllClear ID Protection Services

We have engaged AllClear ID to protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months. Please note that additional steps may be required to activate your phone alerts and monitoring options.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call, 1-855-285-9868 and a dedicated investigator will help you recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical, or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-285-9868 using the following redemption code: Redemption Code.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national consumer reporting companies. Pursuant to the Fair Credit Reporting Act (FCRA), you may obtain a free copy of your credit report online at www.annualcreditreport.com or by calling toll free 1.877.322.8228. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. You may also contact one or more of the three national consumer reporting agencies listed below:

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1.800.685.1111, www.equifax.com

Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742, www.experian.com

TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016, 1.800.916.8800, www.transunion.com

Place a Fraud Alert and Security Freeze

You may obtain information from the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. If you suspect you may be a victim of identity theft you may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies listed above. The agency that you contact will notify the other two agencies. An initial fraud alert lasts 90 days. An extended alert stays on your file for seven years. To place either of these alerts a consumer reporting agency will require you to provide appropriate proof of your identity. If you ask for an extended alert, you will have to provide an identity theft report.

A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze with each consumer reporting company. A consumer reporting agency may charge you a fee of up to \$5 to place a security freeze, although there is typically no charge if you have been the victim of identity theft. Like a fraud alert, they may also require you to provide proof of your identity (such as your name, Social Security Number, date of birth, address, and/or a government issued ID card or a bill).

Additional Steps to Avoid Identity Theft

Respond to any correspondence from the IRS. Contact us immediately if you receive any IRS notices. If your e-filed return is rejected because of duplicate filing under your Social Security Number, file Form 14039, Identity Theft Affidavit with the IRS. Additional information about tax related identity theft is available at: <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. If the IRS contacts you it will always be by mail first, never by e-mail or telephone contact.

Contact your local Social Security Administration office to notify them of any potential identity theft. This is especially important if you are age 62 or older and have not started drawing your Social Security benefits. Additional information regarding your Social Security Number can be found online at: www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number.



Monitor your financial accounts and notify your financial institutions of any unusual activity. If you used direct deposit for income tax refunds, please contact your bank for guidance regarding account security. Please notify your financial institutions of any unusual activity.

Additional State Specific Resources. The following state agencies offer additional information and steps to avoid identity theft:

Maryland Attorney General
Identity Theft Unit
200 St. Paul Pl, 16th Floor
Baltimore, MD 21202
<http://www.oag.state.md.us/idtheft/index.htm>
888.743.0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
<http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>
919.716.6400

Oregon Attorney General
Department of Justice
1162 Court Street NE
Salem, OR 97301
<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>
503.378.4400

Iowa Attorney General
1305 E. Walnut St.
Des Moines, IA 50319
<https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/>
515.281.5164

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
<http://www.riag.ri.gov/ConsumerProtection/About.php>
401.274.4400

Suggestions if You Are a Victim of Identity Theft

File a police report. You can file a report with local law enforcement and ask to obtain a copy of the report to submit to any creditors that require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>.

Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Rutherford, MacDonald & Olson, P.C.

Certified Public Accountants

Processing Center • P.O. BOX 141578 • Austin, TX 78714



01267
TO THE PARENT OR GUARDIAN OF
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

August 23, 2017

Private & Confidential

Dear Parent or Guardian of John:

Re: **Notice of Data Breach**

We value the trust that you have placed in your relationship with Rutherford, MacDonald & Olson, P.C. We know that part of that trust is the expectation that the information that you provide to us will be secure and protected. We take our responsibility in that regard very seriously. That is why we are writing to you. We have discovered that, like many other businesses, government agencies, accounting firms, and tax preparers, we were a victim of unauthorized on-line access to our server.

What Happened? Based on the results of a forensic investigation we confirmed that someone was able to gain unauthorized access to our server in March and April of 2017.

What Information Was Involved? The unauthorized party was able to access our server, which contains, among other things, information relating to client tax returns — including Social Security Number, name, address, telephone number, and other state and federal income tax filing related information. While we do not have specific evidence that your information was fraudulently used, because that possibility exists we are providing you with information regarding this incident in an abundance of caution.

What We Are Doing: We notified all individuals affected, law enforcement, and the United States Internal Revenue Service about the security incident and the confidential data that may have been accessed. As an additional precaution we have engaged AllClear ID to protect your identity for 12 months at no cost to you.

What You Can Do: Please review the recommendations on the following page for steps you can take to protect your personal information and sign up for 12 months of complimentary identity protection services.

For More Information: If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident at 1-855-285-9868. The call center is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time (excluding U.S. holidays). If you require extra assistance, please contact Rutherford, MacDonald & Olson, P.C. by phone at (406) 926-1295 or by email at info@rmo-pc.com with the subject line "Data Breach."

Sincerely,

Rutherford, MacDonald & Olson P.C.

Rutherford, MacDonald & Olson P.C.



01-02-2-00

Important Information: Recommendations You Can Take to Protect Your Identity

Contact AllClear ID Protection Services

We have engaged AllClear ID to protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months. Please note that additional steps may be required to activate your phone alerts and monitoring options.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call, 1-855-285-9868 and a dedicated investigator will help you recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical, or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-285-9868 using the following redemption code: Redemption Code.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national consumer reporting companies. Pursuant to the Fair Credit Reporting Act (FCRA), you may obtain a free copy of your credit report online at www.annualcreditreport.com or by calling toll free 1.877.322.8228. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. You may also contact one or more of the three national consumer reporting agencies listed below:

Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241, 1.800.685.1111, www.equifax.com

Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742, www.experian.com

TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016, 1.800.916.8800, www.transunion.com

Place a Fraud Alert and Security Freeze

You may obtain information from the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. If you suspect you may be a victim of identity theft you may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies listed above. The agency that you contact will notify the other two agencies. An initial fraud alert lasts 90 days. An extended alert stays on your file for seven years. To place either of these alerts a consumer reporting agency will require you to provide appropriate proof of your identity. If you ask for an extended alert, you will have to provide an identity theft report.

A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze with each consumer reporting company. A consumer reporting agency may charge you a fee of up to \$5 to place a security freeze, although there is typically no charge if you have been the victim of identity theft. Like a fraud alert, they may also require you to provide proof of your identity (such as your name, Social Security Number, date of birth, address, and/or a government issued ID card or a bill).

Additional Steps to Avoid Identity Theft

Respond to any correspondence from the IRS. Contact us immediately if you receive any IRS notices. If your e-filed return is rejected because of duplicate filing under your Social Security Number, file Form 14039, Identity Theft Affidavit with the IRS. Additional information about tax related identity theft is available at: <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. If the IRS contacts you it will always be by mail first, never by e-mail or telephone contact.

Contact your local Social Security Administration office to notify them of any potential identity theft. This is especially important if you are age 62 or older and have not started drawing your Social Security benefits. Additional information regarding your Social Security Number can be found online at: www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number.



Monitor your financial accounts and notify your financial institutions of any unusual activity. If you used direct deposit for income tax refunds, please contact your bank for guidance regarding account security. Please notify your financial institutions of any unusual activity.

Additional State Specific Resources. The following state agencies offer additional information and steps to avoid identity theft:

Maryland Attorney General
Identity Theft Unit
200 St. Paul Pl, 16th Floor
Baltimore, MD 21202
<http://www.oag.state.md.us/idtheft/index.htm>
888.743.0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
<http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>
919.716.6400

Oregon Attorney General
Department of Justice
1162 Court Street NE
Salem, OR 97301
<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>
503.378.4400

Iowa Attorney General
1305 E. Walnut St.
Des Moines, IA 50319
<https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/>
515.281.5164

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
<http://www.riag.ri.gov/ConsumerProtection/About.php>
401.274.4400

Suggestions if You Are a Victim of Identity Theft

File a police report. You can file a report with local law enforcement and ask to obtain a copy of the report to submit to any creditors that require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf>.

Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Rutherford, MacDonald & Olson, P.C.
Certified Public Accountants

Stephen L. Rutherford

Terrace West * 619 S.W. Higgins Ave. * Suite R * Missoula, Montana 59803

Gregg N. Olson

Date

Private & Confidential

[Company Name
Address
City, State, Zipcode]

Dear [Name]:

Re: Notice of Security Incident

We value the trust that you have placed in your relationship with Rutherford, MacDonald & Olson, P.C. That is why we are writing to you. We have discovered that, like many other businesses, government agencies, accounting firms, and tax preparers, we were a victim of unauthorized on-line access to our server. We conducted a forensic investigation to help determine what happened. Based on the results of that investigation, we have confirmed that someone was able to access our server which contains, among other things, QuickBooks® databases of past and present clients for whom we provided accounting, tax and payroll services. In many cases, these databases contain personal information including the Social Security Numbers of our client's employees and subcontractors.

Although we do not have evidence that your employees' and/or subcontractors' information was fraudulently used, in an abundance of caution, we plan on notifying them about this situation. Because we maintain their Social Security Number, we will offer them free credit monitoring, identity theft restoration service, and ID theft insurance at our expense. Please see Exhibit A for a copy of the notification letter that we intend to send to them. If you would prefer that we not contact your employees and/or subcontractors, please let us know by September XX, 2017. You can contact us by email at info@rmo-pc.com or by phone at (406) 926-1295.

If you have questions or concerns that are not addressed in this notice letter, please contact Rutherford, MacDonald & Olson, P.C. by phone at (406) 926-1295 or by email at info@rmo-pc.com with the subject line "Security Incident."

Yours truly,

Rutherford, MacDonald & Olson P.C.

Rutherford, MacDonald & Olson P.C.

Exhibit A

Rutherford, MacDonald & Olson, P.C.
Certified Public Accountants

Stephen L. Rutherford

Terrace West * 619 S.W. Higgins Ave. * Suite R * Missoula, Montana 59803

Gregg N. Olson

Date

Private & Confidential

Individual's Name
Address
City, State, Zip code

Dear [Name]:

Re: *Notice of Data Breach*

Rutherford, Macdonald & Olson P.C. provides accounting, tax and/or payroll processing services to [INSERT ENTITY NAME]. Like many other businesses, government agencies, accounting firms, and tax preparers, we recently discovered that our server, which contains your information, including your Social Security Number, was accessed by an unauthorized party. Although we do not have any evidence that your information has been misused, we are notifying you of this situation in an abundance of caution.

What Happened? Based on the results of a forensic investigation we confirmed that someone was able to gain unauthorized access to our server in March and April of 2017.

What Information Was Involved? The unauthorized party was able to access our server, which contains, among other things, QuickBooks® databases of past and present clients for whom we provided accounting, tax and payroll services. In many cases, these databases contain personal information including Social Security Number, name, address, telephone number, and other state and federal income tax filing related information. While we do not have specific evidence that your information was fraudulently used, because that possibility exists we are providing you with information regarding this incident in an abundance of caution.

What We Are Doing: We notified all individuals whose Social Security Number was on our server. We also notified law enforcement about the security incident and the confidential data that may have been accessed. As an additional precaution we have engaged AllClear ID to protect your identity for 12 months at no cost to you.

What You Can Do: Please review the recommendations on the following page for steps you can take to protect your personal information and sign up for 12 months of complimentary identity protection services.

For More Information: If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident at <<DID_PHONE>>. The call center is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time (excluding U.S. holidays).

Sincerely,

Rutherford, MacDonald & Olson P.C.

Rutherford, MacDonald & Olson P.C.

Important Information: Recommendations You Can Take to Protect Your Identity

Contact AllClear ID Protection Services

We have engaged AllClear ID to protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months. Please note that additional steps may be required to activate your phone alerts and monitoring options.

- **AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call <<DID_PHONE>> and a dedicated investigator will help you recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.
- **AllClear Credit Monitoring:** This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical, or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling <<DID_PHONE>> using the following redemption code: REDEMPTION CODE.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national consumer reporting agencies. Pursuant to the Fair Credit Reporting Act (FCRA), you may obtain a free copy of your credit report online at www.annualcreditreport.com or by calling toll free 1.877.322.8228. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. You may also contact one or more of the three national consumer reporting agencies listed below:

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Place a Fraud Alert and Security Freeze

You may obtain information from the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. If you suspect you may be a victim of identity theft you may place a fraud alert in your file by calling one of the three consumer reporting agencies listed above. The agency that you contact will notify the other two agencies. An initial fraud alert lasts 90 days. An extended alert stays on your file for seven years. To place either of these alerts a consumer reporting agency will require you to provide appropriate proof of your identity. If you ask for an extended alert, you will have to provide an identity theft report.

A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze with each consumer reporting company. A consumer reporting agency may charge you a fee of up to \$5 to place a security freeze, although there is typically no charge if you have been the victim of identity theft. Like a fraud alert, they may also require you to provide proof of your identity (such as your name, Social Security Number, date of birth, address, and/or a government issued ID card or a bill).

Additional Steps to Avoid Identity Theft

- **Respond to any correspondence from the IRS.** Contact your tax professionals immediately if you receive or require assistance responding to any IRS notices. Additional information about tax related identity theft is available at: <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. If the IRS contacts you it will always be by mail first, never by e-mail or telephone contact.

- **Contact your local Social Security Administration office to notify them of any potential identity theft.** This is especially important if you are age 62 or older and have not started drawing your Social Security benefits. Additional information regarding your Social Security Number can be found online at: www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number.
- **Monitor your financial accounts and notify your financial institutions of any unusual activity.** If you used direct deposit for pay checks, please contact your bank for guidance regarding account security. Please notify your financial institutions of any unusual activity.
- **Additional State Specific Resources.** The following state agencies offer additional information and steps to avoid identity theft:

Maryland Attorney General
Identity Theft Unit
200 St. Paul Pl, 16th Floor
Baltimore, MD 21202
<http://www.oag.state.md.us/idtheft/index.htm>
888.743.0023

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
<http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>
919.716.6400

Oregon Attorney General
Department of Justice
1162 Court Street NE
Salem, OR 97301
<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>
503.378.4400,

Iowa Attorney General
1305 E. Walnut St.
Des Moines, IA 50319
<https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/>
515.281.5164.

Rhode Island Attorney General
150 South Main St.
Providence, RI 02903
<http://www.riag.ri.gov/ConsumerProtection/About.php>
401.274.4400

Suggestions if You Are a Victim of Identity Theft

- **File a police report.** You can file a report with local law enforcement and ask to obtain a copy of the report to submit to any creditors that require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.pdf>.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Rutherford, MacDonald & Olson, P.C.
Certified Public Accountants

Stephen L. Rutherford

Terrace West * 619 S.W. Higgins Ave. * Suite R * Missoula, Montana 59803

Gregg N. Olson

Date

Private & Confidential

Individual's Name
Address
City, State, Zip code

Dear [Name]:

Re: **Notice of Data Breach**

Rutherford, Macdonald & Olson P.C. provides accounting, tax and/or payroll processing services to [INSERT ENTITY NAME]. Like many other businesses, government agencies, accounting firms, and tax preparers, we recently discovered that our server, which contains your information, including your Social Security Number, was accessed by an unauthorized party. Although we do not have any evidence that your information has been misused, we are notifying you of this situation in an abundance of caution.

What Happened? Based on the results of a forensic investigation we confirmed that someone was able to gain unauthorized access to our server in March and April of 2017.

What Information Was Involved? The unauthorized party was able to access our server, which contains, among other things, QuickBooks® databases of past and present clients for whom we provided accounting, tax and payroll services. In many cases, these databases contain personal information including Social Security Number, name, address, telephone number, and other state and federal income tax filing related information. While we do not have specific evidence that your information was fraudulently used, because that possibility exists we are providing you with information regarding this incident in an abundance of caution.

What We Are Doing: We notified all individuals whose Social Security Number was on our server. We also notified law enforcement about the security incident and the confidential data that may have been accessed. As an additional precaution we have engaged AllClear ID to protect your identity for 12 months at no cost to you.

What You Can Do: Please review the recommendations on the following page for steps you can take to protect your personal information and sign up for 12 months of complimentary identity protection services.

For More Information: If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident at <<DID_PHONE>>. The call center is available Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time (excluding U.S. holidays).

Sincerely,

Rutherford, MacDonald & Olson P.C.

Rutherford, MacDonald & Olson P.C.

Important Information: Recommendations You Can Take to Protect Your Identity

Contact AllClear ID Protection Services

We have engaged AllClear ID to protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months. Please note that additional steps may be required to activate your phone alerts and monitoring options.

- **AllClear Identity Repair:** This service is automatically available to you with no enrollment required. If a problem arises, simply call <<DID_PHONE>> and a dedicated investigator will help you recover financial losses, restore your credit, and make sure your identity is returned to its proper condition.
- **AllClear Credit Monitoring:** This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of credit, criminal, medical, or employment fraud against children by searching thousands of public databases for use of your child's information. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling <<DID_PHONE>> using the following redemption code: REDEMPTION CODE.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national consumer reporting agencies. Pursuant to the Fair Credit Reporting Act (FCRA), you may obtain a free copy of your credit report online at www.annualcreditreport.com or by calling toll free 1.877.322.8228. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. You may also contact one or more of the three national consumer reporting agencies listed below:

- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com
- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com

Place a Fraud Alert and Security Freeze

You may obtain information from the consumer reporting agencies about fraud alerts and security freezes. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. If you suspect you may be a victim of identity theft you may place a fraud alert in your file by calling one of the three consumer reporting agencies listed above. The agency that you contact will notify the other two agencies. An initial fraud alert lasts 90 days. An extended alert stays on your file for seven years. To place either of these alerts a consumer reporting agency will require you to provide appropriate proof of your identity. If you ask for an extended alert, you will have to provide an identity theft report.

A security freeze prohibits a consumer reporting agency from releasing information from your credit report without your prior written authorization, which makes it more difficult for unauthorized parties to open new accounts in your name. The consumer reporting agencies have 3 business days after receiving a request to place a security freeze on a consumer's credit report. Unlike a fraud alert, you must separately place a credit freeze with each consumer reporting company. A consumer reporting agency may charge you a fee of up to \$5 to place a security freeze, although there is typically no charge if you have been the victim of identity theft. Like a fraud alert, they may also require you to provide proof of your identity (such as your name, Social Security Number, date of birth, address, and/or a government issued ID card or a bill).

Additional Steps to Avoid Identity Theft

- **Respond to any correspondence from the IRS.** Contact your tax professionals immediately if you receive or require assistance responding to any IRS notices. Additional information about tax related identity theft is available at: <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>. If the IRS contacts you it will always be by mail first, never by e-mail or telephone contact.

- **Contact your local Social Security Administration office to notify them of any potential identity theft.** This is especially important if you are age 62 or older and have not started drawing your Social Security benefits. Additional information regarding your Social Security Number can be found online at: www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number.
- **Monitor your financial accounts and notify your financial institutions of any unusual activity.** If you used direct deposit for pay checks, please contact your bank for guidance regarding account security. Please notify your financial institutions of any unusual activity.
- **Additional State Specific Resources.** The following state agencies offer additional information and steps to avoid identity theft:

Maryland Attorney General
Identity Theft Unit
200 St. Paul Pl, 16th Floor
Baltimore, MD 21202
<http://www.oag.state.md.us/idtheft/index.htm>
888.743.0023

North Carolina Attorney
General
9001 Mail Service Center
Raleigh, NC 27699
<http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx>
919.716.6400

Oregon Attorney General
Department of Justice
1162 Court Street NE
Salem, OR 97301
<https://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/>
503.378.4400,

Iowa Attorney General
1305 E. Walnut St.
Des Moines, IA 50319
<https://www.iowaattorneygeneral.gov/for-consumers/general-consumer-information/identity-theft/>
515.281.5164.

Rhode Island Attorney
General
150 South Main St.
Providence, RI 02903
<http://www.riag.ri.gov/ConsumerProtection/About.php>
401.274.4400

Suggestions if You Are a Victim of Identity Theft

- **File a police report.** You can file a report with local law enforcement and ask to obtain a copy of the report to submit to any creditors that require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.pdf>.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.