IMPORTANT INFORMATION
PLEASE READ CAREFULLY

Dear [redacted]

The privacy of your personal information is of utmost importance to Next Generation Tax and Accounting (NGTA). I am writing to you with important information about a recent incident that may involve the security of some of your personal information that was supplied to us. We wanted to provide you with information regarding the incident and let you know that we continue to take significant measures to help protect your information.

On February 15, 2016, our information technology vendor detected an unauthorized access to the NGTA server, potentially impacting the security of the information contained within it. We immediately commenced an investigation of the incident and retained an independent computer forensic firm to analyze the extent of the intrusion. After discovering the issue, we promptly changed the password to the impacted server. On February 25, 2016, the forensic investigation concluded that an unauthorized third party had accessed the server.

Since completing the forensic investigation, we have devoted considerable time and effort to determine what exact information may have been contained in the affected server and, as such, at risk of disclosure. We also conducted a sophisticated review of the databases in the server that were forensically identified as having contained personal information to ensure accuracy and confirm those potentially impacted. We can confirm that the compromised server contained your full name, address, and Social Security number and may have included your date of birth and bank account number.

To date, we are not aware of any reports of identity fraud, theft, or other harmful activity related to this incident. However, we are aware of some clients that have reported tax fraud issues—when they filed their tax return, the Internal Revenue Service rejected the filing, stating that someone had already filed their return. At this time, we are unaware of these instances being related to our incident. Moreover, due to the complexity of the intrusion, we cannot conclusively determine whether the unauthorized user actually acquired or viewed any of your personal information. However, out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps that you should take as well.

Enclosed you will find information on enrolling in a 12-month membership of Experian's ProtectMyID® Alert, which we are providing at no cost to you, along with other precautionary measures you can take to help protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis. Since your banking information may have been involved in this incident, we advise you to call your banking institution to determine if you should change your bank account number.

Please accept my sincere apologies, on behalf of NGTA, that this incident occurred. We are committed to maintaining the privacy of our clients' information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of our clients' information, which includes implementation of two-factor authentication and monitoring.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at . This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Saturday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to Next Generation Tax and Accounting. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one-year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by [redacted]
2. VISIT the ProtectMyID Website to enroll: [redacted]
3. PROVIDE your 9-character Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call [redacted] provide Engagement [redacted]

Additional Details Regarding Your 12-Month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes and suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts, including credit, debit, and medical insurance cards; assist with freezing credit files; and contact government agencies.
  - It is recognized that identity theft can happen months and even years after an incident. To offer added protection, you will receive ExtendCARE™, which provides you with the same high level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Immediately covers certain costs, including lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary, intended for informational purposes only, and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.)

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [redacted]

2. Placing a Fraud Alert.

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

3. **Consider Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
www.transunion.com/securityfreeze
1-800-680-7289

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

6. **Reporting Identity Fraud to the IRS.**

If you believe that you are a victim of identity fraud, AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected, or you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: www.irs.gov/pub/irs-pdf/f14039.pdf.
- Call the IRS at (800) 908-4490 to report the situation.

Additional information regarding preventing tax-related identity theft can be found at www.irs.gov/uac/Identity-Protection.

McDonald Hopkins

A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

RECEIVED
APR 20 2016
OFFICE OF CONSUMER PROTECTION

MI 480
15 APR '16
PM 2 L

UNITED STATES POSTAGE
PITNEY BOWES
02 1P $ 000.705
0003184298
MAILED FROM ZIP CODE 48304

Montana Attorney General
Office of Consumer Protection
P.O. Box 200151
Helena, Montana 59620

59620015151