BMB ASSOCIATES
C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
(833) 901-0915
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

September 4, 2020

Dear <<First Name>> <<Last Name>>,

BMB Associates (the "Company") recently learned of a data incident which may have resulted in unauthorized access or acquisition of your personal information. We are providing this notice to inform you of the incident so you can take steps to protect you and minimize the possibility of misuse of your information. We apologize for any inconvenience this may cause you and assure you we are working diligently to resolve this incident.

What Happened
On or about March 16, 2020, the Company discovered some clients had IRS E-file rejections. Based on our investigation, the e-filing rejections was due to fraudulent tax filings by an unauthorized third party who was able to compromise the Company's Intuit ProSeries® service and create a guest account. The Company's IT team was able to discover the hidden guest account and was able to remove it on April 2, 2020.

What Information Was Involved
The Company cannot confirm specifically what information, if any, was compromised by the unauthorized person/s. However, the data elements involved in your tax return may include your name, address, e-mail address, phone number, SSN, financial account information. This may also include your spouse and dependent(s)' name and SSN. If applicable, we also have sent a separate notice to the affected spouse and/or dependent(s) but please share this letter to them as well.

What We Are Doing
Immediately upon discovering the incident, The Company commenced an investigation to determine its scope and identify those affected. We hired a third-party IT company to investigate our system and they determined that the unauthorized person/s created a guest account within the Company's Intuit ProSeries®. The Company immediately deleted the unauthorized guest account and changed all of its passwords. Additionally, we have reported the incident to the Sacramento Valley Hi-Tech Crimes Unit, the Federal Bureau of Investigation ("FBI"), and the Internal Revenue Service ("IRS").

To our knowledge, only a small number of our clients have been affected by this incident, however, we are notifying all of our clients in the abundance of caution. The Company treats all personal information in a confidential manner and are proactive in the careful handling of such information. The Company continues to assess and modify its privacy and data security policies and procedures to prevent similar situations from occurring. We also are assisting affected clients with any IRS filings they need to make to report a fraudulent 2019 filing of their Form 1040.

In addition to providing information below on steps you can take to protect your personal information and reduce the risk of identity theft, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: <<Duration>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do

We prepared the attached sheet which includes several steps you can take to protect of your personal information.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 901-0915 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. We encourage you to take full advantage of this service offering. MyIDCare experts are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is December 4, 2020.

For More Information

If you have questions or concerns, you should call IDExperts at (833) 901-0915. Again, we apologize for this situation and any inconvenience it may cause you.

Sincerely,

Clifford M. Barros, E.A.
BMB Associates

What You Should Do to Protect Your Personal Information

We recommend you remain vigilant and consider taking one or more of the following steps to avoid identity theft, obtain additional information, and protect your personal information:

1. We recommend you closely monitor your financial accounts and access resources concerning identity theft, such as information the Internal Revenue Services has published at: http://www.irs.gov/Individuals/Identity-Protection, and well as https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft. **As discussed in the Taxpayer Guide to Identity Theft, IRS Form 14039 can be filed with the IRS to report potential identity theft concerning your federal taxes. You also may want to check with the state(s) in which you file.**

2. Contacting the nationwide credit-reporting agencies as soon as possible to:

- Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. This statement alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. To place a 90 day fraud alert on your credit file, log into the Equifax Member Center and click on the fraud alert tab, visit www.fraudalerts.equifax.com or call the auto fraud line at 1-877-478-7625, and follow the simple prompts. This fraud alert will remain on your credit file for 90 days.

- Place a "security freeze" on your credit account. This means that your credit account cannot be shared with potential creditors. A security freeze can help prevent new account identity theft. If you would like to request a security freeze be placed on your account, you must write by certified or overnight mail (see addresses below) to each of the three credit reporting agencies, or through the electronic or Internet method made available by the credit reporting agencies. In your request, you also must include (documentation for both the spouse and the victim must be submitted when requesting for the spouse's credit report) (i) a copy of either the police report or case number documenting the identity theft, if you are a victim of identity theft; (ii) your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth; (iii) if you have moved in the past 5 years, the addresses where you have lived over the prior 5 years; (iv) proof of current address such as a current utility bill or phone bill; (v) a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and, if applicable (vi) payment by check, money order or credit card (Visa, Master Card, American Express or Discover cards only.)

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

- Receive a free copy of your credit report by going to www.annualcreditreport.com.

Equifax	Experian	TransUnion
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022
(800) 525-6285	(888) 397-3742	(800) 888-4213
www.equifax.com	www.experian.com/consumer	www.transunion.com

3. The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. You may contact the FTC by visiting www.ftc.gov or www.consumer.gov/idtheft, calling (877) 438-4338, or writing to the FTC at the address below. If you suspect or know that you are the victim of identity theft, you should contact local police and/or your state Attorney General. You can also report such activity to the Fraud Department of the FTC, which will collect all relevant information and make it available to law-enforcement agencies. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

4. If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
5. *For North Carolina Residents*: The contact information for the North Carolina Attorney General is: Address: North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699; Telephone: (919) 716-6400; website: www.ncdoj.com/.