Attachment A
Template Notification Letter

February 28, 2017

[MT RESIDENT NAME]
[CLIENT ADDRESS]
[CITY, STATE ZIP]

Dear [MT RESIDENT NAME]:

At Federal Direct Tax Services ("Federal Direct"), we take the privacy and security of our partners' information seriously. As we previously informed you, despite our best efforts, Federal Direct has been the victim of unauthorized access to our company's information. Specifically, on or about February 2, 2017, Federal Direct discovered that an unauthorized third party launched a cyberattack to attempt to gain electronic access to a group of our partners' Electronic Return Originator (ERO) information. If you are receiving this communication, you are included in this group. Unfortunately, these types of cyberattacks are becoming commonplace, and hackers are growing more sophisticated.

The ERO information that was involved in the incident is attributed to Electronic Filing Identification Number (EFIN) owners, and the unauthorized party potentially accessed your first and last name, date of birth, and Social Security number. There is no evidence that any of our partners' client tax information was targeted, obtained, accessed, or viewed.

Based on our investigation, we have determined that the unauthorized access occurred intermittently beginning in early January 2017. After we identified the incident, we immediately took remediation steps and blocked the unauthorized party's ability to access our partners' information. We promptly called each of our partners to inform them about the incident and sent them a preliminary notification letter. We have begun working with our partners, the Internal Revenue Service (IRS), and tax industry banking partners to mitigate any potential impact. We have also reported the incident to the Federal Bureau of Investigation (FBI) for possible criminal investigation. Further, we have taken several actions to enhance the security of our partners' information. Our own investigation into the incident is ongoing, and we will continue to implement additional security measures as needed.

Even though Federal Direct has no reason to believe that your personal information was targeted or has been used to engage in identity theft, we want to provide you with extra assurance and protection. Accordingly, we have retained LifeLock® to provide one (1) year of complimentary identity theft protection to you. To set up your account with LifeLock, please see the instructions below: **[instructions redacted from template]**

We advise you to remain vigilant for incidents of fraud and identity theft by periodically reviewing your account statements and monitoring free credit reports. If you would like to learn

more about the steps you can take to protect against identify theft or fraud, please review the enclosed "Important Identify Theft Information" materials.

Moreover, if we previously informed you that your IRS e-Services and/or EFIN information may also have been involved in the incident, please take the following steps. As a precautionary measure, we suggest that you promptly reset your IRS e-Services password. If you have used the same or a similar password to access online accounts through other websites, such as banking, commercial, and social media websites, we recommend that you change your password for those other online accounts. Next, we recommend that you contact IRS e-Services at 866-255-0654. Be sure to press 1 at the first prompt, 2 at the second prompt, and 1 at the third prompt to reach an e-Services representative. Please let the representative know that you believe your EFIN number may have been compromised and you would like a new one issued immediately. The IRS can issue a new EFIN to you over the phone.

Once you have your new EFIN, please send it to Federal Direct, and we will transition the new EFIN into your tax software and related bank product registrations. We have reported the exposed EFINs to the IRS, and eventually they will take action to shut off the e-filing ability of these EFINs and require high level validation for obtaining new ones issued through e-Services. You may continue to process returns normally at this point, but when your current EFIN is converted to a new one at the IRS, you may experience an inability to submit e-files for approximately twenty-four (24) hours. This delay only affects your ability to send returns, and you can continue to prepare returns as normal.

As a best practice, please periodically monitor your new EFIN, and any others of yours, through your IRS e-Services account moving forward. Doing so will allow you to verify the total numbers and types of returns filed.

The security of your information is important to Federal Direct, and the safety and well-being of our partners is our highest priority. We apologize for any inconvenience this incident may cause you and thank you for your understanding and cooperation. Please feel free to contact me to learn more about the incident and the personal information we maintain about you or to request any type of assistance. You may reach me at (866) 357-2025.

Sincerely,

Joe Rogers, EA
Federal Direct Tax Services

Enclosure: "Important Identity Theft Information"

Important Identity Theft Information

You can help protect yourself from identity theft or other unauthorized use of personal information by taking some simple steps.

Remain vigilant. We recommend you remain vigilant for possible incidents of fraud and identity theft by reviewing your account statements and monitoring free credit reports. Credit reports can be obtained at:

Equifax
1-800-685-1111
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion
1-800-916-8800
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). More information is available on the FTC's web site, at www.consumer.gov/idtheft. You can also call the FTC at (877) IDTHEFT (438-4338) or write to the FTC at the following address:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Add fraud alerts to your credit file. You can add a fraud alert to your credit report file to help protect your credit information at no charge. 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, but it also may delay your ability to obtain credit. To place a fraud alert in your file, call one of the three nationwide credit bureaus. As soon as that bureau processes your fraud alert, it will notify the other two bureaus, which will also place fraud alerts in your file.

Place a security freeze on your credit report. You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your

name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information about the process:

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
1-888-766-0008

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

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

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.