



22116

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

This notice is a follow-up to the email that we sent on June 4, 2021 notifying you that MLP Tax & Financial Services, Inc. (“MLP”) experienced a security incident that may have involved some of your personal information. We are pleased to inform you that MLP will be offering complimentary identity monitoring services to all potentially affected individuals. Accordingly, we wanted to provide an update on our investigation, what we are doing, and steps you may want to take in response.

What Happened?

As you know, on May 16, 2021, we learned that malicious software code was installed on an employee’s computer. Upon discovery, we immediately took steps to secure the network, protect client data, and begin the restoration process. An outside cybersecurity firm was engaged to help determine what happened, what information was involved, and steps we can take to prevent something like this from happening in the future.

What Information Was Involved?

The investigation was not able to determine which specific emails and files, if any, were viewed by the unauthorized party. However, the affected computer and email account may have contained some of your personal information, including your name, birthdate, Social Security number, and, in very limited cases, bank account numbers.

What We Are Doing.

We want to emphasize that we have no evidence that your specific information was stolen or misused. Our forensic team confirmed that no data from our investment department and no data from prior client databases was compromised. We also contacted our tax software provider, and its auditing division confirmed no unauthorized users were added, no databases were copied or exported, and there was no “outside” normal business hours access that may have signaled a larger security incident.

Our IT provider has removed the malware from the sole infected system and installed additional safeguard programs companywide to prevent this type of crime from happening again. In addition to notifying law enforcement and cooperating with their investigation, we also tightened security protocols, installed additional software safeguards restricting unauthorized updates or installations, and will be adding additional threat detection training for all employees.

We have arranged for you to receive a complimentary two-year membership of identity monitoring services through Kroll. Kroll is a leader in risk mitigation and response, and its team has experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To activate the identity monitoring services being offered at no cost to you, please follow the instructions below:

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information on identity theft and additional steps you may consider taking in response, please see the information provided with this letter.

What You Can Do.

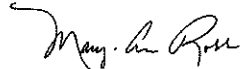
It is always a good idea to remain vigilant by regularly reviewing your financial accounts and credit reports for any unauthorized activity over the next twelve to twenty-four months. If you see charges or activity you did not authorize, please contact your financial professional immediately.

For More Information.

We regret that this occurred and apologize for any inconvenience this incident may have caused. For more information on identity theft prevention and your complimentary services, as well as some additional steps you can take to protect your personal information, please see the additional information enclosed with this letter. If you have questions, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

If there is anything else that we can do to assist you or provide information to file claims, please feel free to contact our office and ask for your assigned tax preparer.

Sincerely,



Principal

MLP Tax & Financial Services, Inc.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and

can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

MLP Tax & Financial Services, Inc. is located at 101 Metro Dr # 650, San Jose, CA 95110.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

Massachusetts: Under Massachusetts law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.