



June 18, 2021

Name
Address
Address
Address

Re: Notice of a Data Breach

Dear Valued Client: <First Name> <Last Name>

Please read this letter in its entirety.

What happened?

We recently became aware of a situation where an unauthorized party accessed one of our company's internal servers and company computers. We discovered this situation on April 27, 2021 and took immediate steps to shut down access to the devices. In addition, we immediately engaged third-party expert assistance to help us investigate, evaluate and respond to the situation.

What information was involved?

Based on their review of the situation and an examination of the impacted computing devices, our forensics specialists have indicated that some personal data belonging to you may have potentially been exposed to the unauthorized intruder. This data may have included personally identifiable information (PII), such as some combination of your fFull nName, Aaddress, Ddate of Bbirth, Social Security Number, and bBanking Iinformation.

While we have no evidence that any of your personal information was compromised or misused in any manner, we are taking appropriate precautionary measures to ensure your financial security and help alleviate concerns you may have.

What are we doing to address this situation?

Weiss & Company has made immediate enhancements to our systems, security and practices. Additionally, we have engaged industry experts to assist us in conducting a full review of our security practices and systems to ensure that appropriate security protocols are in place.

We also are committed to helping those people who may have been impacted by this unfortunate situation. That is why Weiss & Company is providing you with access to [representatives who are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line at 1-800-xxx-xxxx and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.](#)

Formatted: Not Highlight

Formatted: Not Highlight

[Additionally, we are providing you with access to Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Cyber Monitoring* services at no charge. These services provide you with alerts for <service lengths> from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. In addition, we are providing you with proactive fraud assistance to help with any questions that you](#)

Formatted: Font: Not Bold

Formatted: Highlight

Formatted: Font: Not Bold

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

might have or in event that you become a victim of fraud. Triple Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have.

To enroll in Triple Bureau Credit Monitoring* services at no charge, please log on to <URL> and follow the instructions provided. When prompted please provide the following unique code to receive services: <CODE HERE.>

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

For guidance with these services, or to obtain additional information about these services, please call the help line at 1-800-405-6108 and provide the fraud specialist with your unique code. Representatives have been retained to help you with any questions or problems you may encounter, including assisting you with obtaining a credit report and setting up fraud alerts.

Additional steps you can take do to address this situation?

If you choose not to use the services described above, we are strongly urging all clients to consider doing the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)

P.O. Box 4500

Allen, TX 75013

www.experian.com

Equifax (1-800-525-6285)

P.O. Box 740241

Atlanta, GA 30374

www.equifax.com

TransUnion (1-800-680-7289)

P.O. Box 2000

Chester, PA 19016

www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY** obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired clients can access their TDD service at 1-877-730-4204.
- **Upon receipt of your credit report**, we recommend that you review it carefully for any suspicious activity.
- Be sure to promptly report any suspicious activity to Weiss & Company.

IRS strongly advises obtaining an Identity Protections PIN

The Identity Protections ("IP") PIN is a 6-digit number assigned to eligible taxpayers. It helps prevent identity thieves from filing fraudulent tax returns with stolen Social Security numbers (SSNs). An IP PIN also helps the IRS verify taxpayers' identities and accept their electronic or paper tax returns for processing. The IRS issues IP PINs to confirmed identity theft victims once their cases are resolved. This process is unchanged. What is new is that any taxpayers who wants an IP PIN, even if they are not victims of identity theft, may now obtain one as well.

Here's what you need to know before applying for your IP PIN:

- This is a voluntary program.
- You must pass a rigorous identity verification process to obtain an IP PIN.
- Spouses and dependents are also eligible for an IP PIN if they can verify their identities.
- An IP PIN is valid for a calendar year.
- You must obtain a new IP PIN each filing season, using the online IP PIN tool.
- The online IP PIN tool is unavailable generally mid-November through mid-January each year.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

- Correct IP PINs must be entered on electronic and paper tax returns to avoid rejections and delays.

How to Get an IP PIN:

The fastest, easiest and preferred way is by using the **Get an IP PIN** online tool. Here is how it works:

- Go to [IRS.gov/IPPIN](https://www.irs.gov/ippin), select the **Get an IP PIN** tool, verify your identity, and create an account
- Once you have a username, password and security code, you can enter the **Get an IP PIN** tool
- Once in, your IP PIN will be revealed to you.

Unable to pass the online identity proofing?

There are alternatives available, but there will be a delay in obtaining an IP PIN. Here is how it works:

- File a Form 15227 if you have a valid SSN or ITIN, an adjusted gross income of \$72,000 or less, and access to a telephone. An IRS assistor will call you, validate your identity and ensure that you receive an IP PIN the next filing season.
- If you are ineligible for Form 15227, call the IRS to learn about in-person options.

Other important information:

You can also obtain more information about identity theft and ways to protect yourself from the Federal Trade Commission (FTC). The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

For more information:

While representatives should be able to provide thorough assistance and answer most of your questions, you may still feel the need to speak with Weiss & Company regarding this incident. If so, please call me at 858-362-9999 between 9:00 AM and 5:00 PM Pacific Time, Monday through Friday.

At Weiss & Company we take our responsibilities to protect your personal information very seriously. We are deeply disturbed by this situation and apologize for any inconvenience.

Sincerely,

Kenneth L. Weiss
President of Weiss & Company

Commented [AC1]: Do you have an image of Ken's signature or is a script font ok?

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Free Annual Report

P.O. Box 105281
Atlanta, GA 30348
1-877-322-8228
www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney

General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

North Carolina Attorney

General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.