

Parrish Group PS

(Previously Janet Gibb, Gibb + Company PS)

<<Return to Kroll>>

<<Return Address>>

<<City, State ZIP>>

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

PARENT/GUARDIAN OF:

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>

<<ADDRESS_1>>

<<ADDRESS_2>>

<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>

<<COUNTRY>>

NOTICE OF DATA BREACH

Dear Parent/Guardian of <<First_Name>> <<Last_Name>>,

Please read this letter in its entirety.

We are writing to provide you with a formal notification regarding a data incident that occurred at the office of Parrish Group PS, previously known as Janet Gibb, Gibb + Company PS, in which your minor's information may have been accessible to an unauthorized user. This letter serves to provide additional information concerning the incident, what is being done to correct it, and what you can do to further protect your information.

What Happened?

On March 12, 2025, we discovered that an unauthorized user gained access to Janet Parrish's online email account and sent out some fraudulent emails under a deceptive and unauthorized domain. We believe this fraudulent access occurred on or around March 12, 2025. We are providing you with notice so that you may be proactive in protecting your minor's data.

We immediately worked with IT specialists to terminate the threat actor's access and commenced an investigation to determine the cause and scope of the incident. At this time, the investigation has shown that your minor's sensitive information may have been accessible to the threat actor if it was not sent or received in a secure manner. Unfortunately, these types of incidents are becoming increasingly common and organizations with some of the most sophisticated IT infrastructure available continue to be affected.

We have no information that your minor's sensitive data has been misused by the threat actor. That said, we are taking appropriate precautionary measures to protect your minor's financial security and to help alleviate concerns you may have. If we become aware of any suspicious activity in connection with your minor's tax returns, we will notify you immediately. Conversely, if you receive any notifications from the IRS concerning suspicious activity on your minor's account, please notify your tax preparer right away.

What Information Was Involved?

Our investigation has revealed that some sensitive information may have been accessible to the threat actor, such as your minor's social security number, other government identification numbers, name, bank account information, and/or other sensitive information your minor may have also provided to us via email if it was not sent or received in a secure manner.

What We Are Doing.

In response to this incident, we have implemented additional security measures to further protect our network and reduce the risk of a similar incident occurring in the future. We have implemented new software to protect against malware, phishing, and other email-borne threats, as well as implementing a password manager. Finally, we have updated our email archive management policies.

Further, we are working with the appropriate agencies on your minor's behalf. The FBI, IRS, and Secret Service have been notified of this incident. After consulting with the IRS, we implemented their recommended procedures to determine if there was fraudulent activity, and we found none. This notification to you was not delayed as a result of law enforcement investigation if one were to exist.

If we learn that your minor's sensitive information has been compromised beyond that which is available in our email account, we will let you know immediately.

We are taking this matter very seriously and are committed to helping those people who may have been impacted by this unfortunate situation.

What You Can Do.

When sending sensitive, confidential information digitally, be sure to transmit this information through a secure link or portal. If one has not been provided, please request one before sharing sensitive personal information.

Additionally, if you have not done so already, you should do the following:

The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your minor's credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your family member's existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on the credit report for one year. You can renew it after one year:

You can obtain Credit Monitoring for your minor by contacting 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

- Obtain free copies of your minor's credit report and monitor them upon receipt for any suspicious activity.
 - Contact any of these three major credit bureaus to place a free fraud alert on your minor's credit file. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on the credit report for one year, after which you can renew if desired.
 - Be sure to promptly report any suspicious activity to Janet Parrish, CPA.
- We strongly suggest you contact the IRS about getting an Identity Protection PIN to use with your minor's Social Security Number for heightened security. You can do this by going to <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. The initial process to register for the PIN will only take about 10-15 minutes.
 - Remember, the IRS will never call you on the phone to demand information, money, or threaten you with arrest. Any IRS correspondence would be received in the form of a Notice or Letter. Please let us know if you receive any IRS correspondence regarding this incident so we can assist you with the response.
 - Further, we recommend you change any passwords, usernames, or security questions your minor may have shared with us.
 - We strongly recommend you be vigilant in reviewing your minor's bank accounts and other financial account statements, as well as monitoring your minor's Credit Monitoring or free credit reports. Consider notifying your minor's bank(s) and investment advisor(s) to see if they have any suggestions to enhance the security on your accounts.
 - If you suspect fraudulent activity, report it to law enforcement, including the Federal Trade Commission at <https://www.identitytheft.gov/#/> and your State Attorney General's Office at <https://www.naag.org/find-my-ag/>.
 - You can obtain more information from the Federal Trade Commission and your State Attorney General's Office about identity theft, fraud alerts, security freezes, and the protection of your sensitive information. The Federal Trade Commission can be contacted as follows:
 - **Federal Trade Commission**
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-382-4357
<https://www.consumer.ftc.gov/>

For More Information.

We are committed to helping those people who may have been impacted by this unfortunate situation. Protecting your minor's information is incredibly important to us, as is addressing this incident with the information and assistance you may need. If you have questions, please call (866) 559-4615, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Janet Parrish

Janet Parrish