

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY, ESQ.
MFarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Visit us online at
www.C-WLAW.com

Phone: (610) 567-0700

Fax: (610) 567-0712

CONFIDENTIAL ATTORNEY
WORK PRODUCT

July 18, 2024

Via Email

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

RE: Data Breach Notification

To Whom It May Concern:

We serve as counsel for Growth Builders, LLC (“Growth”) located at 740 15th Street NW, Suite 400, Washington, DC 20005. We write to provide notification of a recent data security incident. By providing this notice, Growth does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or about December 5, 2023, Growth identified suspicious activity involving certain services provided by its third-party IT managed services provider, HRTec. At that point, HRTec advised Growth that the issue was resolved. On January 5, 2024, however, Growth began receiving communications from the threat actor(s) directly and recognized that they were victims of a cyber attack due to a shared connection with HRTec, who was the threat actor’s original target. Upon discovery, Growth took immediate action to address and investigate the incident, which included contacting HRTec, and engaging independent third-party forensic specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that, due to Growth’s business relationship with HRTec, an unauthorized actor gained access to certain information on the Growth network for a limited period of time.

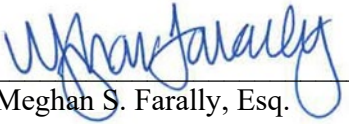
On May 30, 2024, Growth completed its review and determined the type of information affected included full name, Social Security number, passport number, driver’s license number, financial account number, routing number, health insurance information, and medical treatment/diagnosis information Growth identified approximately thirty-nine (39) Maryland residents who may have been impacted by this incident.

In response to this incident, Growth immediately took steps to secure its environment, undertook a thorough investigation, and engaged a new third-party IT services provider. Additionally, they provided notice to the potentially impacted individuals on July 15, 2024 via U.S. mail. A copy of the notices are attached as ***Exhibit A***. In an abundance of caution, Growth is offering the potentially impacted individuals complimentary credit monitoring and identity protection services.

Very truly yours,

CIPRIANI & WERNER, P.C.

By:



Meghan S. Farally, Esq.

Exhibit A



<<Name>>
<<Address 1>>
<<City>>, <<State>> <<ZIP>>



<<Date>>

Dear <<Name>> :

Growth Builders, LLC (“Growth”) writes to inform you of an incident experienced by its former third-party IT services provider, Human Resources Technologies, Inc. (“HRTec”), that may affect the privacy of certain information related to you. We take the privacy and security of all information very seriously and are providing information about the incident, our response, and steps you can take to help protect your information, should you feel it appropriate to do so.

What Happened: On or about December 5, 2023, we identified suspicious activity involving certain services provided by our third-party IT managed services provider, HRTec. Upon discovery, Growth took immediate action to address and investigate the incident, which included contacting HRTec, and engaging independent third-party forensic specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that, due to Growth’s business relationship with HRTec, an unauthorized actor gained access to certain information on the Growth network for a limited period of time. We then began a comprehensive review of the contents of potentially impacted data in order to determine the type(s) of information present and to whom that information related. Growth completed its review on May 30, 2024, and is now providing notification to potentially impacted individuals.

What Information Was Involved: The information identified in our review includes your first and last name, in combination with the following data element(s): <<Data Elements>>.

What We Are Doing: We have taken the steps necessary to address the incident and are committed to fully protecting all of the information entrusted to us. Upon learning of this incident, we immediately took steps to secure our environment, undertook a thorough investigation, and engaged a new third-party IT services provider. Additionally, in an abundance of caution, we are offering you access to complimentary credit monitoring and identity protection services.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanation of benefits forms for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information regarding steps you can take to help protect yourself against fraud and identity theft, including activating the complimentary credit monitoring and identity protection services we are offering.

For More Information: Should you have any questions or concerns, we can be reached at 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays). The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

A handwritten signature in dark ink, appearing to read "E. J. Gorman", with a stylized flourish at the end.

Edward J. Gorman
President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.



How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<<Credit Monitoring Code>>**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports, account statements, and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	--	---

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Growth Builders may be contacted at 740 15th Street NW, Suite 400, Washington D.C. 20005.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. Growth Builders may be contacted at 740 15th Street NW, Suite 400, Washington D.C. 20005.



Parent/Guardian of <<Name>>
<<Address 1>>
<<City>>, <<State>> <<ZIP>>



<<Date>>

Dear Parent/Guardian of <<Name>> :

Growth Builders, LLC (“Growth”) writes to inform you of an incident experienced by its former third-party IT services provider, Human Resources Technologies, Inc. (“HRTec”), that may affect the privacy of certain information provided to us regarding your minor child. We take the privacy and security of all information very seriously and are providing information about the incident, our response, and steps you can take to help protect your minor child’s information, should you feel it appropriate to do so.

What Happened: On or about December 5, 2023, we identified suspicious activity involving certain services provided by our third-party IT managed services provider, HRTec. Upon discovery, Growth took immediate action to address and investigate the incident, which included contacting HRTec, and engaging independent third-party forensic specialists to assist with determining the nature and scope of the incident. A thorough investigation determined that, due to Growth’s business relationship with HRTec, an unauthorized actor gained access to certain information on the Growth network, including human resources and benefits information, for a limited period of time. We then began a comprehensive review of the contents of potentially impacted data in order to determine the type(s) of information present and to whom that information related. Growth completed its review on May 30, 2024, and is now providing notification to potentially impacted individuals.

What Information Was Involved: The information identified in our review of the potentially impacted human resources and benefits information includes your minor child’s first and last name, in combination with the following data element(s): <<Data Elements>>.

What We Are Doing: We have taken the steps necessary to address the incident and are committed to fully protecting all of the information entrusted to us. Upon learning of this incident, we immediately took steps to secure our environment, undertook a thorough investigation, and engaged a new third-party IT services provider. Additionally, in an abundance of caution, we are offering your minor child access to identity protection services.

What You Can Do: We encourage you to enroll in the identity protection services we are making available to your minor child. Information about how to enroll in these services and additional resources available to your minor child is included in the attached *Steps You Can Take to Help Protect Your Minor Child’s Information*. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your minor child’s account statements and explanation of benefits forms for suspicious activity and to detect errors.

For More Information: Should you have any questions or concerns, we can be reached at 1-800-405-6108 Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays). The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

A handwritten signature in dark ink, appearing to read "E. J. Gorman", with a stylized flourish at the end.

Edward J. Gorman
President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR MINOR CHILD'S INFORMATION

Enroll in Identity Protection

In response to the incident, we are providing the parents of impacted minors with access to Cyber monitoring services for you and your minor child for 12 months at no charge. Cyber monitoring will look out for yours and your minor's personal data on the dark web and alert you if their personally identifiable information is found online. These services will be provided by Cyberscout, a TransUnion company,

To enroll in Cyber Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<Credit Monitoring Code>>

Once you have enrolled yourself, click on your name in the top right of your dashboard and select "Manage Family Protection" then "Add Family Member" to enroll your child. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and an email account and will require enrollment by parent or guardian first. 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.

Monitor Accounts

Although minors under the age of 18 typically do not have a credit report, under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place a "security freeze" on the file, which will prohibit a credit bureau from releasing information in the credit file without your express authorization. Pursuant to federal law, you cannot be charged to place or lift a security freeze on a credit file. To request a security freeze for your minor, you will need to provide the following information for both you and your minor:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth; and
4. Address for the prior two to five years

Include for your identification:

5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. Proof that you are the parent or legal guardian of the minor.

Include for you minor's identification:

8. A copy of your minor's Social Security card and
9. A copy of your minor's birth certificate.



00001020280000

P

Should you wish to contact the credit reporting bureaus or place a security freeze, please contact the bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
--	--	---

Additional Information

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect your minor's personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you or your minor ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you or your minor have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>. Growth Builders may be contacted at 740 15th Street NW, Suite 400, Washington D.C. 20005.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>. Growth Builders may be contacted at 740 15th Street NW, Suite 400, Washington D.C. 20005.