

Cynthia J. Larose
617 348 1732
cjarose@mintz.com



MINTZ

One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

September 23, 2021

Via E-MAIL TRANSMISSION (DOJ-CPB@doj.nh.gov)

Attorney General John Formella
Office of the New Hampshire Attorney General
Attn: Security Incident Notification
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Attorney General Formella:

We are writing on behalf of Gulfside Supply, Inc. d/b/a Gulfeagle Supply (the "Company") to advise you of an incident that may affect the security of personal information relating to approximately one (1) New Hampshire resident. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

The Company was alerted on May 5, 2021 that a malicious actor had exploited a vulnerability to gain access to certain Company systems as well as various network resources and files in an apparent ransomware attack. The Company promptly engaged a nationally-known forensics firm to determine the nature and scope of the intrusion, and reported the incident to the FBI. The forensic analysis performed by the Company was not able to determine a root cause of the attack. At that time, the Company was able to restore its files and systems from backups, and none of its recovered assets showed any indications of continued compromise or malicious code, however, the Company continued to monitor for any malicious activity. Through that monitoring, on August 23, 2021, the Company became aware that the attacker accessed files containing personal information, and has worked diligently to identify which files and which individuals may have been affected. As a result of the Company's internal investigation, it was determined that the files accessed by the attacker contained personal information including name, address, driver's license, and Social Security number of certain current and former Company employees, including approximately one (1) New Hampshire resident.

The Company is taking this incident very seriously, and has taken a number of steps to strengthen the protection of personal information and mitigate risk to protect from further types of attacks, including applying software patches, resetting all user credentials, modifying its policies, procedures and system access configurations, and strengthening endpoint detection and response. The Company is also in the process of implementing additional safeguards and continuing with its technical investigation and evaluation of risk mitigation activities. The Company will continue to closely monitor the incident and take further steps as appropriate.

The Company is not aware of any fraudulent use of personal information of the affected New Hampshire residents at this time. The Company is sending the attached notices to affected New Hampshire residents on September 23, 2021, and the Company has arranged to make credit monitoring and identity protection services by IDX available to them at no cost for one (1) year. This includes access to assist individuals with credit restoration, a \$1,000,000 insurance reimbursement policy, and credit monitoring services as described in the attached form of notice.

MINTZ

Office of Attorney General
September 23, 2021
Page 2



Please contact the undersigned at cjarose@mintz.com or 617-348-1732 should you need further information or have any additional questions.

Sincerely,

/s/ Cynthia J. Larose
Member

Attachments

116759365v.1

Gulfside Supply, Inc. d/b/a Gulfeagle Supply
2700 E. 7th Ave.
Tampa, FL 33605

| |
|--|
| To Enroll, Please Call: 1-833-992-3396 Or Visit: https://app.idx.us/account-creation/protect Enrollment Code: <<XXXXXXXXXX>> |
|--|

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

September 23, 2021

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

What Happened

Gulfside Supply, Inc. d/b/a Gulfeagle Supply (“Gulfeagle”) has discovered that an unknown malicious actor gained access to part of Gulfeagle’s network and may have had access to certain files, including some of your personal information. We are writing to provide you with information regarding this incident.

Gulfeagle was alerted on May 5, 2021 that a malicious actor had exploited a vulnerability to gain access to certain Gulfeagle systems as well as various network resources and files, and promptly engaged a nationally-known forensics firm to determine the nature and scope of the intrusion. At that time, we were able to restore our files and systems from backups, and none of our recovered assets showed any indications of continued compromise or malicious code, but we continued to monitor for any activity. Through that monitoring, on August 23, 2021, we became aware that the attacker accessed files containing personal information and we have worked diligently to identify which files and which individuals may have been affected. We have not received any reports of fraudulent use of information accessed by the malicious actor.

What Information Was Involved

The following personal information may have been involved in the incident: name, address, social security number, and driver’s license.

What We Are Doing

We have notified law enforcement and are working to improve security and mitigate risk to protect from further types of attacks. As part of the process, we reset all credentials, applied software patches, and began a comprehensive review of attacker activities. We are also implementing additional safeguards and are continuing with our technical investigation and evaluation of risk mitigation activities to implement further security measures.

In addition, we are offering all potentially impacted individuals identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We are offering these services to comply with law, and in states where laws do not require that we provide such services, we have determined that all potentially impacted individuals receive these services, regardless of your state of residence.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-992-3396 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 AM – 9:00 PM Eastern Time. Please note the deadline to enroll is **December 23, 2021**.

Again, at this time, we have not received any reports or information that your personal information has been misused. However, we encourage you to take full advantage of this service offering.

For More Information

You will find detailed instructions for enrollment on the enclosed Additional Information document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-992-3396 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Brad Resch

Jill Buhler

Brad Resch
President

Jill Buhler
Vice President, HR

(Enclosure)

Additional Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-992-3396 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. It is always a good practice to be vigilant for incidents of fraud by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

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

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

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. You have the right to put a security freeze on your credit file, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. If you place a security freeze on your credit file, 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 security freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting agency.* Federal and state laws prohibit charges for placing, temporarily lifting, or removing a security freeze.

The following information must be included when requesting a security freeze (note that if you are requesting a security freeze for your spouse, this information must be provided for your spouse as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five (5) years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: You have the right to file a police report and obtain a copy of it.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 91 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.