

2020 AUG 26 PM 12:33

Nicholas J. DiCesare

Partner

August 21, 2020

VIA REGULAR MAIL

New Hampshire Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: **DiVal Safety Equipment, Inc.**
Our File No. 3003398

NOTICE OF DATA SECURITY INCIDENT

Dear Sir:

We are counsel to DiVal Safety Equipment, Inc. ("DiVal"). We are writing to inform you of a recent security incident involving DiVal. Specifically, on July 30, 2020, DiVal became aware of ransomware attack on some of its computer systems. Based on the investigation to date, the ransomware has been identified as a type of ransomware called DoppelPaymer. Upon learning of the attack, DiVal immediately engaged forensic experts as well as a ransomware expert to protect and attempt to recover its systems, and to prevent any further access to the information. It appears that as part of the attack the criminals were able to extract some files that did contain protected information, specifically the name, address, and social security number of DiVal employees – one such employee is a resident of New Hampshire. A copy of the notification letter that was sent out to the individuals impacted by the incident is enclosed herewith.

As noted above, DiVal engaged an expert, Coveware, to negotiate with the criminals in an attempt to recover all the files and prevent the posting to the internet; however, they were unable to reach a settlement. As a result, files were posted to the internet on or about August 10, 2020. A few days after the files were posted, the FBI was able to seize the cloud share account that contained the files and remove it from the site.

Please be assured that DiVal has taken, and is continuing to take, this incident very seriously. DiVal has taken numerous steps to protect information and prevent further disclosure. Specifically, DiVal, with the assistance of security experts Fortinet and Global Security IQ, has identified steps to immediately secure its system including the installation of EDR Software on all devices to assist in detecting any future threats. DiVal is continuing to work with these experts to conduct a thorough assessment of data security to ensure there are no additional vulnerabilities. As noted above, DiVal notified law enforcement of the ransomware attack, and we will be notifying all other appropriate government agencies of this incident.

DiVal Safety Equipment, Inc.
Notice of Security Incident
Page 2

Should you have any questions or require anything further, please do not hesitate to contact me.
Thank you for your attention to this matter.

Respectfully,

A handwritten signature in blue ink, appearing to read 'NJD', followed by a long horizontal flourish.

Nicholas J. DiCesare

NJD:
Enclosure

August 20, 2020

NOTICE OF DATA SECURITY INCIDENT

To All DiVal & Galetton Employees:

We are writing to inform you of a recent security incident at DiVal Safety Equipment, Inc. On July 30, 2020, DiVal became aware of ransomware attack on some of its computer systems. Based on the investigation to date, the ransomware has been identified as a type of ransomware called DoppelPaymer. Upon learning of the attack, DiVal immediately engaged forensic experts as well as a ransomware expert to protect and attempt to recover its systems, and to prevent any further access to the information. It appears the criminals were able to extract some files that did contain protected information, such as your name, address, and social security number. As noted above, DiVal engaged an expert to negotiate with the criminals in an attempt to recover all the files and prevent the posting to the internet, however, they were unable to reach a settlement. As a result, files were posted to the internet. A few days after the files were posted, the FBI was able to seize the cloud share account that contained the files and remove it from the site.

Please be assured that DiVal has taken, and is continuing to take, this incident very seriously. We have taken numerous steps to protect your information and prevent further disclosure. Specifically, DiVal, with the assistance of Fortinet and Global Security IQ, has identified steps to immediately secure our system including the installation of EDR Software on all devices to assist in detecting any future threats. DiVal is continuing to work with these experts to conduct a thorough assessment of data security to ensure there are no additional vulnerabilities. We have notified law enforcement of the ransomware attack, and we will be notifying all other appropriate government agencies of this incident.

DiVal is fully committed to assisting you in protecting your identity. To help ensure that your identity and private information are not unlawfully used, we will be offering you identity theft protection through ID SHIELD at no charge. Information regarding the protection, along with meeting dates, is attached.

Additionally, to protect yourself from the possibility of identity theft, we recommend that you place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf.

- Equifax Information Services LLC, P.O. Box 105788, Atlanta, GA 30348-5788, 1-888-298-0045, <https://www.equifax.com/personal/credit-report-services/>

- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, www.experian.com/freeze/center.html
- Trans Union Security Freeze, P.O. Box 160, Woodlyn, PA 19094, 1-800-680-7289, <https://www.transunion.com/credit-freeze>

You can also place a security freeze on your credit reports, also called a credit freeze. A credit freeze helps stop anyone from opening new lines of credit in your name by preventing a credit reporting agency from releasing your credit report to others without written authorization.

Under the law, you cannot be charged to place, lift, or remove a credit freeze. To place a credit freeze on your credit report, you may send a written request by regular, certified, or overnight mail to each of the three major agencies, Equifax, Transunion, and Experian at the addresses above. You may also place a credit freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information noted above.

In order to request a security freeze, expect to provide some or all of the following information to the credit reporting agency, depending on whether you request the freeze online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. Addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Social Security card, pay stub, or W2
8. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit agencies must send written confirmation of the credit freeze to you and should provide you with a personal identification number or password that you will use to temporarily lift or remove a credit freeze. It is important you remember this number or password or put it in a safe place, because you may to give it to the agency if you want to lift the credit freeze.

For additional information about credit freezes, please see the FTC's website at <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

Please note that a credit freeze also stops businesses from checking your credit, so you may need to temporarily lift your credit freeze before: applying for any type of loan, mortgage, or credit card; applying for insurance; switching or starting a new utility service or phone line, including a cell phone; applying for a job; or applying to rent an apartment.

You will also receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each. When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. If you identify any unauthorized activity, you should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Lastly, attached is a supplement that provides some additional information specific to certain localities.

Even if you do not find signs of fraud on these credit reports, we recommend that you remain vigilant in reviewing credit reports from the three major credit reporting agencies as well as your bank and credit card statements for any unusual or unauthorized activity. If you have any questions or concerns, please contact Kristy Paglino, HR Generalist, kpaglino@divalsafety.com, 716-874-9060 Ext# 3138.

Sincerely,

DiVal Safety Leadership Team

SUPPLEMENT TO NOTICE OF DATA SECURITY INCIDENT

FOR RESIDENTS OF MASSACHUSETTS:

In addition to the various resources identified in the Notice, you may also 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

In addition, pursuant to Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

FOR RESIDENTS OF NORTH CAROLINA:

In addition to the various resources identified in the Notice, you may also contact the North Carolina Attorney General's Office, which provides additional information and resources regarding the prevention of identity theft. The contact information for the North Carolina Attorney General's Office is as follows:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

FOR RESIDENTS OF RHODE ISLAND:

In addition to the various resources identified in the Notice, you may also contact and obtain information from your state attorney general at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400
<http://www.riag.ri.gov/>

In addition, pursuant to Rhode Island law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.