

November 15, 2021

Robert Walker
601.499.8083 (direct)
601.499.8077 (main)
Robert.Walker@wilsonelser.com

Via electronic-mail: DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov

Attorney General John M. Formella

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re:	Our Client	:	Dicar, Inc.
	Matter	:	Data Security Incident on September 23, 2021
	Wilson Elser File #	:	16516.01636

Dear Attorney General Formella:

We represent Dicar, Inc. (“Dicar”), located in Pine Brook, New Jersey, with respect to a potential data security incident described in more detail below. Dicar takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that Dicar is taking to restore the integrity of the system. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

It appears that on or around September 23, 2021, Dicar was the target of a cybersecurity incident. An unauthorized third party attempted to infiltrate Dicar’s computer systems. This incident may have resulted in the exposure of personal information that is located on Dicar’s systems, including full name, home address, email address, social security number, and date of birth that could have been located on HR documents.

Dicar, however, is not aware of any evidence that information has been misused. Dicar has not received any reports of related identity theft since the date of the incident (September 23, 2021 to present).

2. Number of New Hampshire Residents Affected

A total of one (1) resident of New Hampshire was potentially affected by this security incident. A notification letter will be sent to this individual on November 16, 2021, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

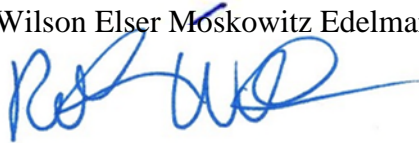
Upon learning of this incident, Dicar moved quickly to institute a response plan, which included conducting an investigation with the assistance of third-party forensic specialists and engaging in steps to confirm the security of any relevant systems. Dicar has reported this incident to law enforcement. Dicar has reviewed, altered and enhanced its policies and procedures relating to the security of its systems and servers, as well as its information life cycle management.

4. Contact Information

Dicar remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.Walker@WilsonElser.com or 601.499.8083.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

A handwritten signature in blue ink, appearing to read 'RW' followed by a stylized flourish.

Robert F. Walker, Esq.
RW / rmc

Copy: Ryan M. Cook, Esq. (Wilson Elser LLP)

Enclosure: *Sample Notification Letter*

Dicar, Inc.

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



Via First-Class Mail

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

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

November 16, 2021

Notice of Data Breach

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

We are writing to inform you of an incident that may have exposed your personal information. We take the privacy of your personal information seriously and want to provide you with information and resources you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

On September 23, 2021, an unauthorized third-party infiltrated our network. Dicar, Inc. ("Dicar") detected and stopped the network security incident by immediately shutting off all access to the network and engaging a highly specialized third-party forensic and technical resources firm to respond to the incident and conduct an investigation. Dicar has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused during the network compromise, an investigation of the incident revealed that your full name, mailing address, birthdate, social security number and email address may have been exposed to the unauthorized third-party.

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate our incident response, which included fully securing and remediating our network and the data that we maintain. We conducted a comprehensive investigation with the assistance of third-party forensic specialists and have reported this matter to law enforcement. We have reviewed and altered our tools, policies, and procedures relating to the security of our systems and servers, as well as our information life cycle management. We have also secured free credit monitoring and identity theft services for all affected individuals, as set forth in full below.

In short, Dicar has taken and will continue to take every reasonable step available to ensure that your personal information is not misused because of the security incident. As of this writing, Dicar has not received any reports of related identity theft since the date of the incident.

What You Can Do:

We value the safety of your personal information and are offering complimentary credit monitoring and identity theft protection services through IDX. IDX's services include: <<12/24>> months of credit and CyberScan monitoring and

fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to remain vigilant against incidents of identity theft and fraud by enrolling in this free identity theft protection and credit monitoring. Contact IDX with any questions and to enroll in these services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX is available Monday through Friday 6am to 6pm Pacific Time. Please note the deadline to enroll is February 16, 2022.

We encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact IDX at the number listed above.

Dicar values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,

A handwritten signature in black ink, appearing to read "Steven A. San Filippo". The signature is fluid and cursive, with a large, stylized "S" at the beginning and a distinct "P" at the end.

Steven A. San Filippo
Chairman
Dicar, Inc.

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her 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 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are located above.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you 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 proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain

further information on how to file such a complaint by way of the contact information listed above. 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us.

For 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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

For 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, and <https://ag.ny.gov/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.