



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 27, 2023

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Zeroed-In Technologies, LLC (“Zeroed-In”), located at 8595 College Parkway, Suite 350, Fort Myers, FL 33919, and are writing on behalf of the below entities to notify your Office of an incident that may affect the security of certain information relating New Hampshire residents. Zeroed-In is a data and technology consulting firm that provides workforce analytical services to its customers, including the following entities (“Customers”) and includes the total number of impacted individuals in parenthesis below:

- Dollar Tree & Family Dollar, 500 Volvo Parkway, Chesapeake, VA 23320, (5,828)

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Zeroed-In does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 8, 2023, Zeroed-In discovered suspicious activity related to certain network systems. Zeroed-In immediately took steps to secure the systems and launched an investigation into the nature and scope of the activity. Through the investigation, it was determined that an unauthorized actor gained access to certain systems between August 7, 2023 and August 8, 2023. While the investigation was able to determine that these systems were accessed, it was not able to confirm all of the specific files that were accessed or taken by the unauthorized actor. Therefore, Zeroed-In conducted a review of the contents of the systems to determine what information was present at the time of the incident, to whom the information relates, and to which Zeroed-In customers the information belonged. This review was completed on August 31, 2023 and Zeroed-In notified Customer of the event because certain individuals associated with them were

identified during the review. The information that was present on the systems at the time of the incident includes . Zeroed-In coordinated notification with Customer and is providing notice to individuals and regulators, as required, on Customer's behalf.

Notice to New Hampshire Residents

On or about November 27, 2023, Zeroed-In began providing written notice of this incident to approximately 5,828 New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Notification to impacted customers and individuals is ongoing, and Zeroed-In may supplement this notification if it is determined that a significant amount of additional New Hampshire residents will receive notice.

Other Steps Taken and To Be Taken

Upon discovering the event, Zeroed-In moved quickly to investigate and respond to the incident, assess the security of Zeroed-In systems, and identify potentially affected individuals and Zeroed-In customers. Further, Zeroed-In notified federal law enforcement regarding the event. Zeroed-In is also reviewing existing policies and procedures and implemented additional safeguards. Zeroed-In is also providing complimentary access to credit monitoring services for through TransUnion, to individuals whose information was potentially affected by this incident.

Additionally, Zeroed-In is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Zeroed-In is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/jlm
Enclosure

EXHIBIT A

Zeroed-In Technologies, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



November x, 2023

NOTICE OF SECURITY INCIDENT

Dear [REDACTED]:

Zeroed-In Technologies, LLC ("Zeroed-In") is writing to notify you of a security incident that involved your information. Zeroed-In is a data and technology consulting firm that provides workforce analytical services to its clients, including [REDACTED]. As part of these services, Zeroed-In receives information related to applicants and current and former employees of its clients. This letter includes information about Zeroed-In's response to the incident and additional steps you may consider taking.

What Happened? On August 8, 2023, Zeroed-In discovered suspicious activity related to certain systems. Zeroed-In immediately took steps to secure the systems and launched an investigation into the nature and scope of the activity. Through the investigation, we determined that an unauthorized actor gained access to certain systems between August 7, 2023, and August 8, 2023. While the investigation was able to determine that these systems were accessed, it was not able to confirm all of the specific files that were accessed or taken by the unauthorized actor. Therefore, Zeroed-In conducted a review of the contents of the systems to determine what information was present at the time of the incident and to whom the information relates.

What Information Was Involved? This review was completed on August 31, 2023, and Zeroed-In notified [REDACTED] of this incident. We are notifying you because the investigation determined that your information was present on the systems involved at the time of the incident and the information includes

What We Are Doing. Zeroed-In takes the confidentiality, privacy, and security of information in our care very seriously. Upon discovering the event, we took steps to secure our systems, launched an investigation, and reported this event to federal law enforcement. As part of our ongoing commitment to the security of your information, we are reviewing our existing policies and procedures and implemented additional safeguards to prevent a similar event from occurring in the future. Zeroed-In is also reporting this event to relevant regulators, as required.

Zeroed-In is also offering you 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 twelve (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 through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. You must activate these services and instructions to do so can be found in the enclosed *Additional Steps You Can Take*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed *Additional Steps You Can Take*, which includes further information on additional steps you may

000010102G0500

P


consider taking. Additionally, Zeroed-In encourages you to activate the complimentary credit monitoring being offered.

For More Information. Zeroed-In understands you may have questions about this event that are not addressed in this letter. If you have additional questions, please contact our dedicated assistance line 1-833-930-1130 Monday through Friday from 8:00 am to 8:00 pm Eastern time, excluding holidays. You may also write to Zeroed-In at 8595 College Parkway, Suite 350, Fort Myers, FL 33919

We sincerely apologize for any inconvenience this may cause.

Sincerely,

Zeroed-In Technologies

Para obtener una versión en carta en español, visite: 

ADDITIONAL STEPS YOU CAN TAKE

Enroll in Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/zeroedintech> and follow the instructions provided. When prompted please provide the following unique code to receive services: XXXXXXXXXX

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

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1- year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094



Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General.

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.

For New York residents, you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 7485 Rhode Island residents that may be impacted by this event.