MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

November 21, 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 Incident

To Whom It May Concern:

We represent NSC Technologies located at 1200 Ashwood Parkway, Suite 590, Atlanta, GA 30338, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately eight (8) New Hampshire residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, NSC Technologies 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 Incident

On June 26, 2023, NSC Technologies became aware of potential suspicious activity within its computer systems. Upon learning of the activity, NSC Technologies quickly took steps to confirm the security of its systems and with the assistance of external cybersecurity specialists, began a comprehensive investigation to determine the full nature, scope, and impact of the activity. The investigation determined that NSC Technologies was the victim of a sophisticated cyberattack and an unauthorized actor likely acquired certain files stored on NSC Technologies systems between June 19, 2023, and June 20, 2023. NSC Technologies subsequently conducted a thorough and time-consuming review of the files likely affected to determine whether they contained any sensitive information and to whom the information relates. This review recently concluded on November 1, 2023, and thereafter NSC Technologies worked to provide notice to affected individuals as quickly as possible.

The information present in the files that were potentially impacted by this event includes

Notice to New Hampshire Residents

On or about November 21, 2023, NSC Technologies provided written notice of this incident to approximately eight (8) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the incident, NSC Technologies moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, NSC Technologies notified federal law enforcement regarding the incident. NSC Technologies continues to review and enhance its existing policies and procedures relating to data protection and security. NSC Technologies has also implemented additional security measures to mitigate risk associated with this incident and to help prevent future similar incidents. NSC Technologies is providing access to credit monitoring services for , through IDX, A ZeroFox Company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, NSC Technologies is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. NSC Technologies is providing individuals with 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.

NSC Technologies is providing written notice of this incident to relevant state regulators, as necessary.

Contact Information

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

Very truly yours,

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ/dle
Enclosure

EXHIBIT A

NSC
The Skilled Staffing Experts™
P.O. Box 989728
West Sacramento, CA 95798-9728

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

November 21, 2023

<<Variable Data 4 (Variable Header)>>

Dear <<First Name>> <<Middle Initial>> <<Last Name>>:

NSC Technologies writes to inform you of an incident that may impact the privacy of some of your information. You are receiving this letter because you previously applied to or were employed by NSC Technologies or one of its subsidiaries which include Anistar Technologies, Consolidated Marine Systems, Nationwide Temporaries, Staffing Resources, Staff Matters, Superior Resource Group, and ULG Companies. Although we have no indication that your information has been misused as a result of the incident, we are providing you with information about the incident, our response to it, and steps you can take in addition to those you take every day to protect your personal information, should you feel it appropriate to do so.

What Happened? On June 26, 2023, we became aware of potential suspicious activity within our computer systems. Upon learning of the activity, we quickly took steps to confirm the security our systems and with the assistance of external cybersecurity specialists, began a comprehensive investigation to determine the full nature, scope, and impact of the activity. We also promptly notified federal law enforcement. The investigation determined that NSC Technologies was the victim of a sophisticated cyberattack and an unauthorized actor likely acquired certain files stored on our systems between June 19, 2023, and June 20, 2023. We subsequently conducted a thorough and time-consuming review of the files likely affected, to determine whether they contained any sensitive information and to whom the information relates. This review recently concluded on November 1, 2023, and we determined that your information was in the files that may have been acquired without authorization.

What Information Was Involved? We have no evidence of any actual or attempted misuse of your personal information. The information present in the files that were potentially impacted by this event included

What We Are Doing. We responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice. As part of our ongoing commitment to the privacy and security of personal information in our care, we continue to review and enhance our existing policies and procedures relating to data protection and security. We have also implemented additional security measures to mitigate risk associated with this incident and to help prevent similar future incidents. We are also providing notice of this incident to potentially impacted individuals and to regulators where required.

Out of an abundance of caution, we are providing you with <<Variable Data 5: CM Length>> months of complimentary access to credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services through IDX, A ZeroFox Company, as well as guidance on how to better protect your information, should you feel it is appropriate to do so. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. Although there is no evidence of any actual or attempted misuse of your information, as a general best practice, 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. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring services and how to enroll.

For More Information. If you have questions about this incident, please call our dedicated assistance line at: 1-888-996-3951, Monday through Friday from 9 am to 9 pm Eastern Time. You may also write to us directly at 1200 Ashwood Parkway, Suite 590, Atlanta, GA 30338.

Sincerely,

NSC Technologies

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Complimentary Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/nsctechnologies and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the enrollment deadline is .

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 1-888-996-3951 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. We recommend that you remain vigilant 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.

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) 442-9828; 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 https://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, 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 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 thirteen Rhode Island residents that may be impacted by this event.