



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

December 19, 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 Kimco Staffing Services Inc. (“Kimco”), located at 17872 Cowan Avenue, Irvine, CA 92614, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately three (3) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Kimco 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 or about June 24, 2023, Kimco became aware of suspicious activity related to certain Kimco computer systems. Kimco immediately launched an investigation with the assistance of third-party forensic specialists to secure its network and to determine the nature and scope of the activity. Through the investigation, on August 1, 2023, it was determined that there was unauthorized access to a limited number of systems on Kimco’s network resulting in unauthorized access to data. On November 28, 2023, Kimco completed an internal review of the potentially accessed data and determined what individuals were potentially impacted as a result of this event. Therefore, Kimco is providing this notice in an abundance of caution because of the uncertain nature of the event.

The information that could have been subject to unauthorized access includes

Notice to New Hampshire Residents

On or about December 19, 2023, Kimco provided written notice of this incident to approximately three (3) 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 event, Kimco moved immediately took steps to secure our network and maintain operations in a safe and secure fashion. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on our systems. Kimco is providing access to credit monitoring services for through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Kimco is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Kimco 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.

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,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/cob
Enclosure

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Kimco Staffing Services (“Kimco”) values our relationship with every employee and maintaining your trust and confidence is important to us. We are writing to inform you that our organization recently experienced a cybersecurity event. We are writing today to inform you about what happened, what information was involved, what we have done to address the situation and what you can do to help protect yourself against possible misuse of information.

What Happened? On or about June 24, 2023, we became aware of suspicious activity related to certain Kimco computer systems. We immediately launched an investigation with the assistance of third-party forensic specialists to secure our network and to determine the nature and scope of the activity. Through the investigation, it was determined that there was unauthorized access to a limited number of systems on Kimco’s network on June 24, 2023; however, we were unable to confirm what specific information, if any, may have been impacted due to the unavailability of certain data. Therefore, we are providing this notice in an abundance of caution because of the uncertain nature of the event.

What Information Was Involved? The information impacted varied by individual. The information that may have been impacted includes your

What We Are Doing. Kimco takes the security of your information seriously. Upon learning of this incident, we immediately took steps to secure our network and maintain operations in a safe and secure fashion. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional administrative and technical safeguards to further secure the information on our systems.

In addition, we are offering identity monitoring services through Kroll, a data breach and recovery services expert. Kroll’s identity monitoring services offered by Kimco include: 12 months of credit monitoring. You will find detailed instructions for activation on the enclosed Recommended Steps document.

What You Can Do. While there is currently no evidence that your information has been misused, we recommend that you remain vigilant, monitor and review all of your financial and account statements and explanations of benefits, and report any unusual activity to the institution of record and to law enforcement. You may also review the guidance contained in *Recommended Steps to help Protect Your Information*. You may also in activate the complimentary identity monitoring services offered by Kimco.

For More Information For assistance with questions regarding this incident, please call [TFN] from Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. You may also write to Kimco HR at 17872 Cowan Avenue, Irvine, CA 92614.

Sincerely,

Kimco Staffing Services

Recommended Steps to help Protect your Information

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

*Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 promptly 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; 1-410-528-8662 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 \[xx\] Rhode Island residents that may be impacted by this event.](#)