MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

411 Theodore Fremd Avenue
Suite 206 South
Rye, NY 10580

July 14, 2023

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

To Whom It May Concern:

We represent Kleinberg, Kaplan, Wolff & Cohen, P.C. ("KKWC") located at 500 5th Avenue, New York, New York 10110, and are writing to notify your office of an incident that may affect the security of certain personal information relating to four (4) New Hampshire residents. The investigation into this matter recently concluded. By providing this notice, KKWC 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 December 1, 2022, KKWC determined that there had been temporary unauthorized access to one KKWC attorney's email account stemming from a phishing incident. KKWC began an investigation to assess the incident's scope, including engaging third-party specialists to assist with the response. KKWC also notified law enforcement. The unauthorized email access activity was identified to have occurred from September 6 to 8, 2022, and there is no evidence of unauthorized access beyond the one email account. Based on the available information, the identified activity appears consistent with an attempt to induce third parties to wire payments to non-KKWC bank accounts, and not theft of personally identifiable information or client confidential information.

Out of an abundance of caution, KKWC engaged third-party specialists to conduct a programmatic and manual review of the contents of the affected email account to determine the types of protected personal information present at the time of the incident and to whom the information related. Upon completion of the third-party review, KKWC then undertook a thorough and time-intensive secondary review of the results, including to ascertain up to date address information for the

identified individuals, as well as the names of the clients and third-party organizations with whom they were associated. That review concluded on or about June 30, 2023, and KKWC has moved quickly to notify their clients, the third-party organizations, and the associated individuals to whom the information relates.

The information that could have been subject to unauthorized access varies by individual and may include

Notice to New Hampshire Residents

On behalf of the already-contacted clients and third-party organizations, where applicable, KKWC plans to provide written notice of this incident to the identified individuals on about July 14, 2023, of whom there are four (4) New Hampshire residents. A sample of that individual notice is attached here as ***Exhibit A***. KKWC has notified impacted clients and third-party organizations for whom there were associated individuals with potentially affected personal information and, in certain circumstances, is requesting that these clients/organizations provide address information for those individuals. Certain clients are still gathering address information, and additional notifications to individuals may occur going forward. As such, KKWC may supplement this notification if it is determined that a significant amount of additional New Hampshire residents will receive notification.

Other Steps Taken and To Be Taken

Upon discovering the event, KKWC moved quickly to investigate and identify potentially affected individuals. Further, KKWC has taken steps to further strengthen and enhance the security of systems in its network, including updating administrative and technical safeguards, as well as providing additional cybersecurity training for our personnel. KKWC also notified federal law enforcement. KKWC is providing access to complimentary credit monitoring services for through IDX, to individuals whose personal information was potentially affected by this incident.

Additionally, KKWC is providing identified individuals with a toll-free number, as well as a monitored email address, in the event that they have questions about the incident. The letters being mailed to individuals contain 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. KKWC 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,

Michele Veltri of
MULLEN COUGHLIN LLC

MTV/jlm
Enclosure

EXHIBIT A

KLEINBERG KAPLAN

4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

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

July 14, 2023

NOTICE OF <<SECURITY INCIDENT / DATA BREACH>>

Dear <<First Name>> <<Last Name>>:

Kleinberg, Kaplan, Wolff & Cohen, P.C. ("KKWC") is contacting you regarding an email phishing incident that may have resulted in exposure of some of your personal information. We take the confidentiality, security, and privacy of your information very seriously and for that reason want you to understand what happened, what we are doing to address this incident, and what steps you can take to further protect yourself, should you feel it necessary to do so. While we are unaware of any actual or attempted misuse of your personal information, we are offering complimentary credit monitoring and identity theft protection services as a precaution. Instructions on how to enroll are provided below.

What Happened?

We are a law firm in New York that provides professional services to clients, and in that capacity, we receive and maintain certain information on password-protected systems on behalf of our clients and various other third parties. On December 1, 2022, we determined that one attorney's email account had been temporarily accessed without authorization due to a phishing incident. We began an investigation to assess the incident's scope and engaged third-party specialists to assist with the investigation. We also notified federal law enforcement. The unauthorized access involved one email account and was identified to have occurred from September 6 to 8, 2022. The identified activity appears to have been focused on inducing third parties to wire payments to non-KKWC bank accounts, and not theft of personally identifiable information or client confidential information.

What Information Was Involved?

The affected email account contained personal information and confidential information of clients and other third parties. Out of an abundance of caution, we commenced a review of the contents of the email account to identify the potentially impacted personal information and individuals to whom the personal information may relate, engaging external support to assist with the review and locating up-to-date address information for identified individuals. The review recently concluded, and we are notifying you now because we determined that some of your personal information was in the affected email account. This information may have included . Again, we are unaware of any actual or attempted misuse of your personal information, and there is no evidence of unauthorized access beyond the one identified email account.

What We Are Doing.

As noted above, we engaged third-party specialists to assist with our investigation of the incident and analysis of the email account's contents. We also notified federal law enforcement. In addition, we have taken steps to further strengthen and enhance the security of systems in our network, including updating administrative and technical safeguards, as well as providing additional cybersecurity training for our personnel.

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 also review the enclosed *Steps You Can Take To Protect Personal Information* for additional information on steps you can take to further protect your information, should you feel it necessary to do so. As an added precaution, we are offering you 24 months of complimentary credit monitoring through IDX, A ZeroFox Company. Please review the enrollment instructions included in the attached *Steps You Can Take To Protect Personal Information* and use Enrollment Code <<XXXXXXXX>>. We encourage you to enroll in these monitoring services, as KKWC is not able to do so on your behalf. Please note the deadline to enroll is October 14, 2023.

For More Information.

We apologize for any inconvenience or concern this incident may cause. Security remains a top priority at KKWC, and we will continue to take all appropriate steps to safeguard personal information and our systems. You understandably may have questions that are not addressed in this letter. You may direct any questions you have about the incident to , or call us toll-free at 1. All inquiries will be treated as confidential unless you direct us otherwise.

Sincerely,

Andrew M. Chonoles
Managing Partner

IDX
A ZEROFOX COMPANY

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

1. Website and Enrollment. Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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 1-800-939-4170 to 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.

You should also know that you have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

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, you may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia 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/. KKWC is located at 500 5th Avenue, New York, New York 10110.

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 Oregon residents, we encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; (877) 877-9392 (toll-free in Oregon), (503) 378-4400; or www.doj.state.or.us.

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. On or about June 30, 2023, our investigation concluded that the data security incident described above potentially involved personal information of two Rhode Island residents. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request for a security freeze on your account.