Paul T. McGurkin, Jr.
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

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

February 28, 2024

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notifications
1305 E. Walnut Street
Des Moines, IA 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Houser LLP ("Houser") located at 9970 Research Drive, Irvine, CA 92618 and are writing to notify your office of an incident that may affect the security of certain personal information relating to one thousand four hundred ninety-six (1,496) Iowa residents. By providing this notice, Houser does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

Houser provides legal services to commercial businesses and financial institutions. Houser was provided certain sensitive information from clients to provide such services.

On May 9, 2023, Houser discovered that certain files on their computer systems had been encrypted. Houser immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that there was unauthorized access to the Houser network between May 7, 2023, and May 9, 2023, during which time certain files were copied and taken from the network. However, in June 2023, the unauthorized actor informed Houser that they deleted copies of any stolen data and would not distribute any stolen files.

Houser retained a vendor to conduct a comprehensive review of the files potentially copied to determine whether these files contained any sensitive information. This process was resource intensive and involved multiple steps to ensure the accuracy and completeness of the review. On January 18, 2024, the review was completed by the vendor. Our firm then analyzed the data and provided Houser with the results. Upon receipt of this file, Houser began notifying its clients of the investigation and findings and offered to mail letters to potentially impacted individuals on behalf of these clients. Houser then worked with clients to develop a plan to provide notice to impacted individuals affiliated with its clients.

The information that could have been subject to unauthorized access for Iowa residents includes name and one or more of Social Security number, driver's license number, financial account information, and medical information.

Notice to Iowa Residents

On February 28, 2024, Houser provided written notice of this incident to one thousand four hundred ninety-six (1,496) Iowa 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, Houser moved quickly to investigate and respond to the incident, assess the security of Houser systems, and identify potentially affected individuals. Further, Houser notified the FBI regarding the event. Houser has implemented additional safeguards and policies and procedures relating to data privacy, security and its network environment. These additional safeguards include, but are not limited to, deployment of RocketCyber, an endpoint detection and response tool. Houser has also implemented multi-factor authentication for Outlook 365, net extender VPN tunnel and remote desktop connection. Houser has also added ransomware detection software, implemented the use of phishing simulation software and conducted vulnerability assessment and penetration testing. Houser is providing access to credit monitoring services for twelve (12) months, through IDX, a ZeroFox Company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Houser 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. Houser is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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.

Houser 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 (267) 930-4788.

Very truly yours,

Paul T. McGurkin, Jr. of
MULLEN COUGHLIN LLC

PTM/ekw

EXHIBIT A

HOUSER

PO Box 480149
Niles, IL 60714

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/houser

February 28, 2024

RE: Notice of Data <<Variable Data 2>>

Dear <<Name 1>>,

Houser LLP ("Houser") writes to notify you of an incident that may affect the privacy of some of your information. Houser provides legal services to commercial businesses and financial institutions. Houser was provided your information to provide such services. This letter includes details of the incident, our response, and steps you may take to better protect against possible misuse of your information, should you feel it appropriate to do so.

What Happened? On May 9, 2023, Houser discovered that certain files on their computer systems had been encrypted. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that there was unauthorized access to our network between May 7, 2023, and May 9, 2023, during which time certain files were copied and taken from our network. However, in June 2023, the unauthorized actor informed us that they deleted copies of any stolen data and would not distribute any stolen files.

We then retained a vendor to conduct a comprehensive review of the files potentially copied to determine whether these files contained any sensitive information. This process was resource intensive and involved multiple steps to ensure the accuracy and completeness of the review. On January 18, 2024, the review was completed by the vendor. We then determined that the impacted files contained certain information related to you.

What Information Was Involved? Houser determined that the following information related to you was present within the potentially affected files: your name and <<Variable Data 1>>.

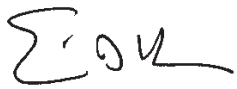
What Houser Is Doing. Houser takes the confidentiality, privacy, and security of information in our care seriously. Upon discovery, we immediately commenced an investigation to confirm the nature and scope of the incident. We reported this incident to law enforcement. We also took steps to implement additional safeguards policies and procedures relating to data privacy, security and our network environment. These additional safeguards include, but are not limited to, deployment of RocketCyber, an endpoint detection and response tool. We also implemented multi-factor authentication for Outlook 365, Net Extender VPN tunnel and remote desktop connection. We also added ransomware detection software, implemented the use of phishing simulation software and conducted vulnerability assessment and penetration testing.

As an added precaution, we are also offering you complimentary access to <<Membership Offering Length>> of credit monitoring and identity theft restoration services through IDX, A ZeroFox Company. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached S*teps You Can Take to Protect Personal Information* for additional information on these services.

What You Can Do. Houser encourages you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. You can also review the enclosed *Steps You Can Take to Protect Personal Information* for general guidance. In addition, you can enroll in the complimentary credit monitoring and identity protection services being offered through IDX.

For More Information We understand that you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call 1-888-910-0969, Monday through Friday, from 8:00 a.m. to 8:00 p.m. Central Time. We sincerely regret any inconvenience that this event may cause you.

Sincerely,



Eric Houser
Managing Partner
Houser LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services

1. **Website and Enrollment.** Scan the QR image or go to https://response.idx.us/houser and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is May 28, 2024.

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 1-888-910-0969 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit 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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. 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 and your 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, DC 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, 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 bureaus 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 violator. 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 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, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this incident.