

Melissa K. Ventrone
T (312) 360-2506
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

August 9, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown,

We represent Tobin, Carberry, O'Malley, Riley & Selinger, P.C. ("TCORS") with respect to a cybersecurity event involving personal information. TCORS is a business associate as defined under the Health Insurance Portability and Accountability Act ("HIPAA") and is providing notice on behalf of certain covered entities. TCORS takes the security of the information in its system seriously and is committed to answering any questions you may have regarding this event.

1. Nature of security incident.

TCORS is a law firm that performs various financial recovery services on behalf of hospitals and hospital systems. On November 30, 2023, TCORS discovered suspicious activity on its systems. TCORS immediately implemented its incident response protocols, contacted law enforcement, and hired external computer forensic specialists and other consultants to assist with an investigation to determine what occurred and whether any data may have been compromised. The investigation determined that TCORS was the victim of a ransomware attack. On February 13, 2024, the investigation found that personal information had most likely been taken from the TCORS system.

TCORS worked to identify potentially impacted covered entities and between February 13-16, 2024 notified them of the security incident and the potential impact to personal information. On April 12, 2024, TCORS posted notice of the security incident on its website and notified the Department of Health and Human Services Office of Civil Rights. During this period of time, TCORS continued to work with its third-party vendors to compile the necessary information to create a data file necessary to mail letters to impacted individuals.

Because of the complexity of the potentially impacted data, TCORS has been pursuing multiple workstreams to be able to assist the covered entities with notifying the impacted population. The first phase was recently completed, enabling TCORS to provide impacted covered entities with a preliminary list of impacted individuals. TCORS recently completed the second phase, which involves reviewing potentially compromised documents and extracting any personal information that may be present.

The affected personal information may contain names and some combination of the following: address, date of birth, Social Security number, diagnosis information, treatment information, health insurance information, medical history and, for a limited number of individuals, bank account information.

2. Number of residents affected.

A total of eight (8) individuals whose personally identifiable information ("PII") was impacted were notified on behalf of YNHH. A letter was sent to the affected individuals on July 19, 2024. See Exhibit A for a copy of the of the template notification letter.

3. Steps taken in response to the incident.

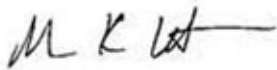
Since this incident, TCORS has deployed enhanced endpoint monitoring software for all endpoints, performed a global password reset for all users, changed the user's password, emphasized additional security training and awareness, and implemented additional security controls. TCORS is also working with a cybersecurity firm to assess its information security controls and is committed to continually improving its security posture. Additionally, potentially affected individuals were offered 12 months of credit monitoring and identity protection services through IDX at no cost.

4. Contact Information

TCORS takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone', with a horizontal line extending to the right.

Melissa K. Ventrone

Yale
NewHaven
Health
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/tcors>

<<First Name>> <<Last Name>> or <<Full Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

July 19, 2024

Dear <<First Name>> <<Last Name>> or <<Full Name>>:

Yale New Haven Health (“YNHHS”) values and respects the privacy of the information that we maintain for our patients, which is why we are writing to advise you of a recent security incident at one of our service partners, Tobin, Carberry, O’Malley, Riley & Selinger, P.C., which may have involved some of your personal information. We are writing to provide you with details of the incident and resources you may utilize, should you feel it is appropriate to do so.

What Happened? On December 4, 2023, one of our vendors, Tobin, Carberry, O’Malley, Riley & Selinger, P.C. (“TCORS”) notified us that it had experienced a security incident. TCORS was engaged to assist our patients in qualifying for Medicaid and long-term care benefits and coverage. TCORS, with the assistance of third-party forensics specialists, conducted a forensic investigation to determine the nature and scope of the incident. Their investigation determined that an unauthorized third-party accessed its network from November 10, 2023, to November 30, 2023, and copied certain files from TCORS systems, including information related to individuals receiving care at YNHHS facilities. On February 13, 2024, TCORS provided notice of the security incident to YNHHS. On May 8, 2024, TCORS provided a list of individuals whose information may have been stored in the copied files.

What Information Was Involved? The copied files contained your address, date of birth, Social Security number, diagnosis information, treatment information, health insurance information, medical history and, for a limited number of individuals, bank account information, and name. Additionally, personal information for members of your household may have been affected if their information was provided in connection with your application(s) for Medicaid or long-term care benefits. Notably, YNHHS has no evidence that your information, or the information of other individuals in your household, has been misused for the purposes of identity theft or fraud.

What We Are Doing. While this incident did not occur at YNHHS, YNHHS regularly implements measures to reduce the risk of this type of incident occurring at our facilities.

Although we are not aware of any instances of fraud or identity theft involving this information, we are offering a complimentary <<one year/two year>> membership of identity theft protection services through IDX, a ZeroFox Company, to you and members of your household (2 adults and up to 5 minors). This product helps detect possible misuse of personal information and provides identity protection services focused on immediate identification and resolution of identity theft. Enrollment is completely free, and enrolling in this program will not negatively affect credit scores. **For more information on IDX, including instructions on how to activate your complimentary membership, please see the additional information provided with this letter. Please note that the deadline to enroll is October 19, 2024.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring through IDX. Information is included in a separate document enclosed with this letter. We also encourage you to carefully monitor the

transactions within your financial accounts and those reflected in your credit report. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please go to <https://response.idx.us/tcors> or call 1-888-804-6081 from 9 a.m. – 9 p.m. Eastern, Monday through Friday.

Sincerely,

A handwritten signature in black ink, reading "Sherry Coomes". The signature is fluid and cursive, with the first name "Sherry" and last name "Coomes" clearly distinguishable.

Sherry Coomes

Chief Compliance and Privacy Officer

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/tcors> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Note, only one adult can use the enrollment code above. Once you have enrolled, you can add a second adult and up to five minors by going to the account detail tab and adding them under Family Management. The second adult will receive an invite to setup their own member portal and the minors will be listed under the account that used the enrollment code.

2. Credit Monitoring Activation. 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 1-888-804-6081 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com/protectYourIdentity.action.

Credit and Security Freezes: By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get

access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742

<https://www.experian.com/freeze/center.html>

P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872

<https://www.transunion.com/credit-freeze>

P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: We believe that this incident affected 689 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

Yale
NewHaven
Health
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/tcors>

July 19, 2024

<<First Name>> <<Last Name>> or <<Full Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Dear <<First Name>> <<Last Name>> or <<Full Name>>:

Yale New Haven Health (“YNHHS”) values and respects the privacy of your information, which is why we are writing to advise you of a recent security incident at one of our service partners, Tobin, Carberry, O’Malley, Riley & Selinger, P.C., which may have involved some of your personal information. We are writing to provide you with details of the incident and resources you may utilize, should you feel it is appropriate to do so.

What Happened? On December 4, 2023, one of our vendors, Tobin, Carberry, O’Malley, Riley & Selinger, P.C. (“TCORS”) notified us that it had experienced a security incident. TCORS was engaged to assist our patients in qualifying for Medicaid and long-term care benefits and coverage, and processing workers compensation claims. TCORS, with the assistance of third-party forensics specialists, conducted a forensic investigation to determine the nature and scope of the incident. Their investigation determined that an unauthorized third-party accessed its network from November 10, 2023, to November 30, 2023, and copied certain files from TCORS systems, including information related to individuals receiving care at YNHHS facilities. On February 13, 2024, TCORS provided notice of the security incident to YNHHS. On May 8, 2024, TCORS provided a list of individuals whose information may have been stored in the copied files.

What Information Was Involved? The copied files contained your address, date of birth, Social Security number, diagnosis information, treatment information, health insurance information, medical history, and name. Notably, YNHHS has no evidence that your information has been misused for the purposes of identity theft or fraud.

What We Are Doing. While this incident did not occur at YNHHS, YNHHS regularly implements measures to reduce the risk of this type of incident occurring at our facilities.

We are offering a complimentary <<one year/two year>> membership of identity theft protection services through IDX, a ZeroFox Company, to you. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Enrollment is completely free to you, and enrolling in this program will not negatively affect your credit score. **For more information on IDX, including instructions on how to activate your complimentary membership, please see the additional information provided with this letter. Please note that the deadline to enroll is October 19, 2024.**

What You Can Do. We encourage you to take advantage of the complimentary credit monitoring through IDX. Information is included in a separate document enclosed with this letter. We also encourage you to carefully monitor the transactions within your financial accounts and those reflected in your credit report. You can find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. We value the trust you place in us to protect your privacy, take our responsibility to safeguard your personal information seriously, and apologize for any inconvenience this incident might cause. For further information and assistance, please go to <https://response.idx.us/tcors> or call 1-888-804-6081 from 9 a.m. – 9 p.m. Eastern, Monday through Friday.

Sincerely,

A handwritten signature in black ink, reading "Sherry Coomes". The signature is fluid and cursive, with the first name "Sherry" and last name "Coomes" clearly distinguishable.

Sherry Coomes
Chief Compliance and Privacy Officer

ACTIVATING YOUR COMPLIMENTARY CREDIT MONITORING

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/tcors> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Credit Monitoring Activation. 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 1-888-804-6081 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: By law, you may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies. The three national credit reporting agencies have also agreed to provide free weekly online credit reports. You can obtain your free credit report by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>. Alternatively, you may elect to purchase a copy of your credit report by contacting the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax
1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
1-888-397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: By law, you have the right to place a fraud alert on your credit report if you believe you have been, or are about to become, a victim of fraud or related crime. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com/protectYourIdentity.action.

Credit and Security Freezes: By law, you have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax Security Freeze
1-888-298-0045
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
<https://www.experian.com/freeze/center.html>
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
<https://www.transunion.com/credit-freeze>
P.O. Box 160
Woodlyn, PA 19094

This notification was not delayed by law enforcement.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New Mexico Residents: Individuals have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.

Oregon Residents: Oregon residents are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General. Oregon residents can contact the Oregon Attorney General at 1162 Court St. NE, Salem, OR 97301-4096; 503-378-4400; <https://www.doj.state.or.us/>.

Rhode Island Residents: We believe that this incident affected 689 Rhode Island residents. Rhode Island residents can contact the Office of the Attorney general at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. You have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).



Melissa K. Ventrone
T (312) 360-2506
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

August 30, 2024

VIA ELECTRONIC MAIL

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown,

We represent Tobin, Carberry, O'Malley, Riley & Selinger, P.C. ("TCORS") with respect to a cybersecurity event of which we originally notified you on August 9, 2024. Prior notices were provided on behalf of TCORS clients. TCORS, on behalf of itself, is now notifying five (5) individuals whose personally identifiable information was impacted. A copy of the template letter is attached as Exhibit A.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'M K Ventrone'.

Melissa K. Ventrone

TCORS
ATTORNEYS
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/tcors>

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

August 30, 2024

NOTICE OF DATA SECURITY <<BREACH/INCIDENT>>

Dear <<First Name>> <<Last Name>>,

Tobin, Carberry, O'Malley, Riley & Selinger, P.C. ("TCORS") is writing to let you know about a data security incident that may have affected some of your personal information that was in our files. TCORS is a law firm, and, as such, may have received some of your personal information if you were a client of TCORS or involved in a matter that TCORS handled.

We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On November 30, 2023, we discovered suspicious activity on our systems. We immediately implemented our incident response protocols, began an investigation, and engaged independent computer forensic experts to assist. In January 2024, the investigation determined that an unauthorized actor gained access to our systems through a device managed by a third party and that some data may have been impacted. We then began working with another vendor to determine what personal information may have been affected. This was a very detailed and time-consuming process. On August 1, 2024, we determined that some of your personal information may have been impacted.

What Information Was Involved?

From our review, it appears that your name and some combination of the following was impacted: <<Variable Text 1>>. While we have no indication that the unauthorized actor actually reviewed or misused any personal information, out of an abundance of caution, we wanted to let you know about this incident and provide you with resources to protect yourselves.

What We Are Doing:

Since the incident, we have changed all passwords and deployed an advanced endpoint and detection monitoring software. In addition, while we are not aware of any misuse of your information, we have arranged for you to receive credit monitoring and identity protection services at no cost to you.

This identity theft protection service is offered through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12/24 months>> of credit and CyberScan monitoring, a

\$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

Again, at this time, there is no evidence that any personal information has been misused by the unauthorized actor. However, we encourage you to contact IDX with any questions and to enroll your family in the free identity protection services by calling 1-888-804-6081, going to <https://response.idx.us/tcors>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 19, 2024.

You should also review the enclosed information, which describes additional steps that can be taken to protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also regularly review your credit reports and financial statements, and immediately report any suspicious activity.

For More Information:

If you have questions, please call 1-888-804-6081, Monday through Friday from 9 am - 9 pm Eastern Time or go to <https://response.idx.us/tcors>. Please have your membership number ready. Protecting your information is important to us and we sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Tobin, Carberry, O'Malley, Riley & Selinger, P.C.

Recommended Steps to Help Protect Your Information

1. Website and Enrollment. Scan the QR image or go to <https://response.idx.us/tcors> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Credit Monitoring Activation. 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 1-888-804-6081 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.

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.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well.

You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will

need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 agencies 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 a 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. You can 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. Total Rhode Island residents notified is 706.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.