



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

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

July 26, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Rogers Towers, P.A. ("Rogers Towers") located at 1301 Riverplace Blvd., Suite 1500, Jacksonville, Florida 32207, and write to notify your office of an incident that may affect the security of certain personal information relating to eight (8) Maryland residents. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Rogers Towers does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 19, 2023, Rogers Towers identified unusual activity in its network. In response, Rogers Towers promptly took steps to secure its network and commenced an investigation into the nature and scope of the activity. On or around January 25, 2023, the investigation identified certain files that may have been viewed on or copied from the Rogers Towers system as part of a cyber incident between January 10 and January 19, 2023. Rogers Towers therefore promptly commenced a thorough review of those files to determine what information was present and to whom the information relates. While these effort were ongoing, based on a preliminary review, on or around February 22, 2023, Rogers Towers identified certain individuals whose personal information was present in the relevant files. On or about March 10, 2023, Rogers Towers began providing written notice of this incident to those individuals whose information was identified at that time. Working with third party data review specialists, Rogers Towers continued to conduct a detailed review of the files at issue to identify any personal information that was present. On or around June 20, 2023, the data review identified an additional set of personal records that was present in the relevant files. Rogers Towers is currently undertaking efforts to review and reconcile those records with its internal files to identify contact information and working to provide notice to those individuals as those efforts progress. The personal information present in the relevant files may include name and Social Security number.

Notice to Maryland Residents

On or about July 26, 2023, Rogers Towers will begin providing written notice of this incident to approximately eight (8) Maryland 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

Rogers Towers takes the confidentiality and security of information very seriously. Upon discovering the incident, Rogers Towers promptly took steps to secure its network and commenced a comprehensive investigation to confirm the nature and scope of the incident. Additionally, Rogers Towers reviewed its existing policies, processes, and security measures and implemented additional safeguards. Rogers Towers is also providing potentially impacted Maryland residents with access to identity monitoring services for one (1) year, through Kroll, at no cost to the individual.

Rogers Towers is also providing potentially affected individuals with guidance on how to better protect their personal information, including 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.

Rogers Towers is also 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) 930-4773.

Very truly yours,



M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/cml
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>>

<<btb_text_1 (RE: Notice of Data Incident/RE: Notice of Data Breach)>>

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

Rogers Towers P.A. (“Rogers Towers”) is writing to make you aware of an incident potentially involving your personal information. This letter contains information about what happened, our response, and the resources available to assist you with safeguarding your information, should you feel it appropriate to do so.

What Happened? In mid-January 2023, Rogers Towers identified unusual activity in its network. In response, we promptly took steps to secure our network and commenced an investigation into the nature and scope of the activity. Through this investigation, we learned that certain files may have been copied from our systems as part of a cyber incident between January 10 and January 19, 2023. We then undertook a detailed review of all files potentially affected by this incident to determine what information was present and to whom it relates. You are receiving this letter because on or around June 20, 2023, we determined that your information was present in the relevant files.

What Information Was Involved? Based on our investigation to date, we determined that the personal information present may include your <<b2b_text_2(full name and data elements)>>.

What We Are Doing. Rogers Towers takes this incident and the privacy of information in its care seriously and conducted a thorough investigation to confirm the full nature and scope of the incident. In response to this incident, we took prompt steps to secure our network in conjunction with conducting a comprehensive investigation. We also reported this incident to federal law enforcement and applicable state regulators.

Further, as part of our ongoing commitment to the privacy and security of information in our care, we reviewed our existing policies, processes, and security measures and implemented additional safeguards. As an added precaution, we are providing you with access to identity monitoring services for one (1) year at no cost to you. Information on these services and instructions on how to activate may be found in the enclosed *Steps You Can Take to Help Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitor your free credit reports for suspicious activity and to detect errors. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Personal Information*.

For More Information. We understand you may have additional questions not addressed by this letter. If you have questions, please contact our dedicated call center at (866) 674-9065, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time (excluding major U.S. holidays). Please have your membership number located on the following page ready.

We regret any inconvenience or concern caused by this incident.

Sincerely,

Rogers Towers

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Activate your Identity Monitoring Services

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. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, 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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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
888-298-0045	888-397-3742	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

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 Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and www.marylandattorneygeneral.gov/. Rogers Towers is located at 1301 Riverplace Blvd # 1500, Jacksonville, FL 32207.

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 event. There is 1 Rhode Island resident potentially impacted by this incident.



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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.