RKPT | ROBBINS KELLY PATTERSON TUCKER
A Legal Professional Association

Michael R. Yeazell, Esq.
myeazell@rkpt.com

<Date>

VIA U.S. MAIL
<Name>
<Address>
<City>, <State> <ZIP>

NOTICE OF DATA BREACH

Dear <Name>,

At Robbins, Kelly, Patterson & Tucker, we take seriously our relationship with you, and for that reason we are reaching out with information on a cyber-attack we experienced in December. In this day and age, cyber-attacks are becoming more and more frequent, and no entity can be 100% protected against all attacks. Rest assured that we have further enhanced the measures we already had in place in response to this incident. And we do not believe your personal information is at risk of misuse.

WHAT HAPPENED
Despite the security measures we had in place, an unauthorized third party gained access to a limited portion of our computer system in early December 2021. After experiencing issues with our computer network, we quickly engaged industry experts to assist in our response and help us determine the scope of the incident. We took measures to terminate the third party's access to our systems and restore the affected portion of our systems—which did not materially impact our ability to operate and provide services. We then retained a data-review firm to help determine whether personal information had been impacted by the incident. On April 7, 2022, we received their results, and we are now providing you notice to give you more information on what happened and our response.

WHAT INFORMATION WAS INVOLVED
As part of the operation of our firm, we collect and maintain various types of personal information, which may include your full name, contact information, Social Security number, driver's license number, medical information, and information related to financial accounts (such as your bank account number or credit card number). The unauthorized third-party may have accessed that information. At this time, we do not believe your information is at risk of misuse. But, in recognition of the importance of your relationship with us, we are offering a complimentary subscription to IdentityWorks—a credit-monitoring service provided by Experian.

WHAT WE ARE DOING
As noted, we hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information. We also notified the FBI, which did not delay this notice. Since then we have continued to assess the scope of the incident and determine whether personal information may have been impacted. We also continue to look for additional safeguards to further enhance our security.

WHAT YOU CAN DO
Unfortunately, in today's world cyber incidents are a regrettably common occurrence despite precautions. As we continue to look for ways to further enhance our network security, we encourage you to also take action to protect your information. At the end of this letter you will find additional information on steps you can take, along with instructions for activating your complimentary credit monitoring.

FOR MORE INFORMATION
Should you have any questions or concerns, we have established a toll-free phone number (866) 902-2385 that we encourage you to call with any questions.

Sincerely,

Michael R. Yeazell

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary two-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by:** August 6, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <code>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by August 6, 2022, and provide them engagement number B053399.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/DataBreach.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.