CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

MEGHAN S. FARALLY
mfarally@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

April 28, 2023

Via E-Mail (IDTheft@oag.state.md.us)
Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Booth & Cook, P.A. ("Booth & Cook") located at 3030 Starkey Boulevard, Suite 100, Trinity, Florida 34655 and write to inform you of a data security incident. By providing this notice, Booth & Cook does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On July 1, 2022, Booth & Cook discovered suspicious activity related to one employee email account. Upon discovery, Booth & Cook took swift action to secure its email system and network. Booth & Cook also reported this incident to law enforcement, launched an internal investigation, and engaged leading, independent cybersecurity specialists to investigate the full scope of this incident. Based on the investigation, Booth & Cook confirmed that one employee email account was subject to unauthorized access between April 26, 2022 and July 1, 2022. In addition to the employee email account, the forensic investigation revealed that certain network files were subject to unauthorized access between May 6, 2022 and July 1, 2022. Booth & Cook's review of the files subject to unauthorized access was completed on November 15, 2022. There were no Maryland residents in that initial population.

Concurrent with the review related to the network files, Booth & Cook also began a thorough review of the contents of the email account subject to unauthorized access to determine the type of information contained in the account and to whom that information related. Booth & Cook then undertook a comprehensive and time-consuming review of its internal records in order to obtain address information for those potentially affected.

Booth & Cook's review of the contents of the impacted email account was completed on February 13, 2023. At that time, it was determined that information related to 1 Maryland resident was potentially subject to unauthorized access. The information believed to potentially be at risk includes a first and last name, in combination with a Social Security number, financial account information and payment card information.

On April 6, 2023, Booth & Cook sent written notice of this incident to the potentially impacted Maryland resident pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,

Meghan Farally, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A

BOOTH COOK
ATTORNEYS AT LAW

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(NOTICE OF DATA BREACH - CA residents only)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to inform you of a data security incident experienced by Booth & Cook, P.A. ("Booth & Cook") that may have involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, this letter includes information about the incident and steps you can take to help protect your information.

What Happened: On July 1, 2022, we discovered suspicious activity related to one employee email account. Upon discovery, we took swift action to secure our email system and network. We also reported this incident to law enforcement, launched an internal investigation, and engaged leading, independent cybersecurity specialists to investigate the full scope of this incident. Based on the investigation, we confirmed that one employee email account was subject to unauthorized access between April 26, 2022 and July 1, 2022. We then began a thorough review of the contents of the email account to determine the type of information contained within the account and to whom that information related. We additionally undertook a comprehensive and time-consuming review of our internal records in order to obtain address information for those potentially affected. This process was completed on February 13, 2023. We are now notifying those individuals whose information was contained within the affected email account and, therefore, are potentially impacted by this incident.

What Information Was Involved: The type of information contained within the email account included your first and last name, in combination with the following data element(s): <<b2b_text_2(data elements)>>.

What We Are Doing: We have taken every step necessary to address the incident and are committed to fully protecting all of the information that you have entrusted to us. Upon learning of this incident, we took the steps described above, including performing password resets. We have also implemented additional technical safeguards to further enhance the security of information in our possession and prevent similar incidents from happening in the future. Out of an abundance of caution, we have arranged for you to activate, at no cost to you, identity monitoring services for 12 months provided by Kroll. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary identity monitoring services is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can activate to receive the complimentary identity monitoring services we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at (866) 869-0375, 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 ready. You may also write to us at 3030 Starkey Blvd, Suite 100, Trinity, Florida 34655.

The security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

Kristina Hudson

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

KROLL

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

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.

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.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;

6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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 fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. 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; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Booth & Cook, P.A. may be contacted at 3030 Starkey Blvd, Suite 100, Trinity, Florida 34655.

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.