Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, TX 75270
lfunk@constangy.com
Direct: 248.709.9385

July 21, 2023

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Constangy, Brooks, Smith & Prophete, LLP represents Topping, Kessler & Co. ("Topping Kessler"), a CPA firm that provides tax preparation and consulting, auditing, accounting, payroll and business advisory services based in Hollywood, Florida, in conjunction with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification law.

1. Nature of the Security Incident

At the end of March 2023, Topping Kessler became aware of a number of unauthorized tax filings for 2022 associated with some of its clients. Topping Kessler immediately took steps to secure the network environment and engaged a cybersecurity firm to conduct an investigation. The investigation determined that an unknown actor gained access to the Topping Kessler network on February 17, 2023 and may have obtained certain client data from the Topping Kessler's Axcess database on or about May 3, 2023. Topping Kessler subsequently initiated a comprehensive review of the affected files to determine whether they contained personal information belonging to individuals. After a thorough investigation, on June 28, 2023, Topping Kessler determined that certain personal information was involved in the incident and worked diligently to notify these individuals.

2. Type of Information and Number of Maryland Residents Affected

Topping Kessler is notifying two (2) residents of Maryland of this data security incident via first class U.S. mail on July 21, 2023. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included name and Social Security number, driver's license or state identification number, date of birth, medical information, health insurance information, and account information. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Topping Kessler reported this incident to the Federal Bureau of Investigation's Internet Crime Complaint Center and has cooperated with investigative efforts in an attempt to hold the perpetrator(s) of this incident responsible, if possible. Topping Kessler has also implemented additional security features in an effort to prevent a similar incident from occurring in the future. Further, as referenced below Topping Kessler has offered all individuals whose information was involved 12 months of complimentary services through IDX, which includes credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, fully-managed identity theft recovery services, and 90 days access to a call center.

4. Contact Information

Topping Kessler remains dedicated to protecting the personal information in its possession. Should you have any questions or need additional information, please do not hesitate to contact me at 248.709.9385 or by e-mail at lfunk@constangy.com.

Best Regards,

Laura K. Funk of CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Encl.: Consumer Notification Letter Sample

TOPPING KESSLER
Certified Public Accountants
4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

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

July 21, 2023

Subject: Notice of Data <<Variable Text 1: Security Incident/Breach>>

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

We are writing to inform you of a data security incident that may have involved your personal information. Topping, Kessler & Co. ("Topping Kessler") takes the privacy and security of personal information very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? At the end of March 2023, Topping Kessler became aware of a number of unauthorized tax filings for 2022 associated with some of its clients. Topping Kessler immediately took steps to secure the company's network environment and find out what happened. The investigation revealed that an unknown actor gained access to and obtained data from our network. On June 28, 2023, we learned that your information may have been involved in the incident. Out of an abundance of caution, we are providing you with this notification and complimentary credit monitoring. Cybersecurity incidents like this are not limited to Topping Kessler and are a widespread issue across all industries. Nevertheless, we want to provide you with information on how to protect your personal information.

What Information Was Involved? The information involved may include your name and your <<Variable Text 2: PI involved>>.

What We Are Doing. As soon as we discovered the incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We notified federal law enforcement and will provide whatever cooperation is necessary to hold the perpetrators accountable. Additionally, Topping Kessler is offering you complimentary credit monitoring and identity protection services for <<Variable Text 3: 12/24>> months through IDX, a national leader in identity protection services. The IDX services, which are free to you upon enrollment, include a subscription for the following: credit monitoring, CyberScan dark web monitoring, fully managed identity recovery services, and $1 million in identity theft insurance coverage. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. You can also enroll in the IDX identity protection services, which are offered to you at no cost.

To receive credit monitoring services, you must be over the age of 18 and have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file.
To enroll in the services provided through IDX, please call 1-800-939-4170, Monday through Friday from 8:00 am – 8:00 pm Central Time, visit https://app.idx.us/account-creation/protect or scan the QR code and insert the Enrollment Code provided above.

Please note the deadline to enroll in these complimentary services is October 21, 2023. Please do not discard this letter, as you will need the Enrollment Code provided above to access services.

For More Information. If you have questions about this letter or need assistance, please call IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 8:00 am – 8:00 pm Central Time. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We sincerely regret any anxiety caused by this incident.

Sincerely,

Topping, Kessler & Co.

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 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 this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov; https://oag.dc.gov/

California: The California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; http://oag.ca.gov/

Maryland: The Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us; https://www.marylandattorneygeneral.gov/

North Carolina: The North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; https://ncdoj.gov/

New York: The New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

Rhode Island: The total number of individuals receiving notification of this incident is 5. The Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, http://www.riag.ri.gov

Texas: The Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: The Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov; https://ago.vermont.gov/