



Sean B. Hoar
Constangy, Brooks, Smith & Prophete, LLP
Cybersecurity & Data Privacy Team
4800 SW Meadows Road, Suite 300
Lake Oswego, Oregon 97035
SHoar@constangy.com
503.459.7707

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

February 21, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony G. Brown
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 Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents Harris Beach PLLC (“Harris Beach”) headquartered in Pittsford, NY in connection with an incident described below. This notice is being sent pursuant to Md. Code Ann., Comm. Law § 14-3504.

1. Nature of Incident

On October 24, 2023 and October 30, 2023, two Harris Beach workstations were accessed without authorization via phishing attacks. The attacks resulted in a legitimate remote solution software being used by an unauthorized actor. The actor accessed files on each local device and a portion of a limited use staging server. Each access lasted approximately one and a half hours and no access credentials were impacted.

On December 8, 2023, Harris Beach determined that certain personal data may have been accessed by the unauthorized actor. After a subsequent digital forensics investigation, followed by extensive automated data mining of user accounts and potentially affected devices, and a thorough manual review of potentially affected data, on or about February 15, 2024, Harris Beach identified individuals whose information was contained within the potentially affected data. The potentially affected information included names, Social Security numbers and/or medical information.

2. Number of Affected Maryland Residents

Harris Beach notified seven (7) Maryland residents of the incident via first class U.S. mail on February 21, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Responding to Incident

Upon discovering the issue, Harris Beach took the steps described above, provided notification to affected clients, retrained the impacted users, reported the matter to the FBI, enhanced technical safeguards to mitigate the likelihood that a similar incident could happen in the future, and notified potentially affected individuals. Harris Beach is also offering affected Maryland residents 12 months of complimentary credit monitoring, identity theft protection, a \$1,000,000 identity theft insurance reimbursement policy, and fully managed identity theft recovery services.

4. Contact Information

If you have any questions or need additional information, please do not hesitate to contact me at 503.459.7707 or shoar@constangy.com and Sebastian Fischer at 202.748.6544 or smfischer@constangy.com.

Sincerely,



Sean B. Hoar
Partner and Chair, Constangy Cyber Team

Encl. Sample Notification Letter



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

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

Subject: Notice of Data Security Incident

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

I am writing to inform you of a data security incident that may have affected your personal information. At Harris Beach PLLC, we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to protect your personal information, and offering you complimentary identity monitoring services.

What Happened. On December 4, 2023, we were informed that certain data may have been accessed without authorization. We immediately began an investigation to determine what, if any, information had been affected. We engaged digital forensics experts to assist with this process. The investigation determined that certain personal information may have been acquired without authorization. After a thorough review of those files, on or about February 15, 2024, some of your personal information was identified as being contained within those files.

What Information Was Involved. The information may have included your <<b2b_text_1 (Data Elements)>>.

What We Are Doing. As soon as Harris Beach discovered the incident, we took the steps described above. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable, and worked with our digital forensics experts to address the root cause of the incident. In addition, 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, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. 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>>

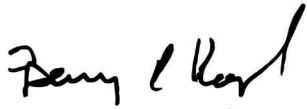
For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What You Can Do. We recommend that you review and implement the guidance included with this letter about how to help protect your information. We also encourage you to activate the services offered to you through Kroll.

For More Information. Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call (866) 992-9469 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Barry Kozak". The signature is fluid and cursive, with the first name "Barry" and last name "Kozak" clearly distinguishable.

Barry Kozak
Chief Operating Officer
Harris Beach PLLC

Steps You Can Take to Protect Your Personal 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 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 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).

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 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
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 2000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. 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>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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. 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.

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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcftp_consumer-rights-summary_2018-09.pdf.



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.