

June 15, 2023

Jonathan L. Wilson

VIA email to idtheft@oag.state.md.us
Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

1800 K Street NW Suite 1000
Washington, D.C. 20006
t 202.783.8400
dd 202.662.4863
f 202.783.4211
jlwilson@shb.com

RE: The Hatcher Agency Data Security Incident

Dear Sir/Madam:

Shook, Hardy & Bacon L.L.P. (“Shook”) represents The Hatcher Agency (“Hatcher”), an insurance agency based in Little Rock, Arkansas. I write to notify you that Hatcher was the victim of a cyber-attack that resulted in an attacker gaining access to a small amount of its data.

Hatcher was the target of a cyber-attack in February 2023. In summary, a threat actor gained access to the laptop of a single Hatcher employee on February 14, 2023. Hatcher discovered the attack on March 14, 2023 when it received an email from a threat actor claiming to have acquired certain data. Hatcher immediately engaged Shook, and we, in turn, immediately engaged a leading digital-forensics firm to assist us in the investigation. Based on our investigation to date, we believe the threat actor had access for roughly an hour on February 14, 2023. Once we identified the data that may have been affected, we immediately engaged a data-review firm to determine what personal information, if any, was in those files. We received the results of that review in early May. Since then, we have been diligently working with Hatcher to identify the correct addresses for the affected individuals and assess Hatcher’s notification obligations.

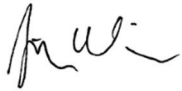
Having reviewed the data, we now have reason to believe that the threat actor potentially accessed the personal information of 10 Maryland residents, whom Hatcher is notifying in accordance with state law. The threat actor may have accessed files containing some combination of the following: full names, contact information, date of birth, government identification (such as a driver’s license or Social Security number), health insurance information, and a limited of medical information. At this time, we have no reason to believe the information was, or will be, misused.

Hatcher will began notifying the potentially affected individuals on June 16, 2023 and we have attached a template of those notification letters. In the letter, as you will see, Hatcher provides the individual with one year of free credit-monitoring and identity theft protection services and a toll-free call center has been set up to field any questions individuals have about the incident. We are also sending a letter to the three main Consumer Reporting Agencies (Experian, TransUnion, and Equifax) about the incident.

In addition to providing notice, Hatcher has taken a variety of measures to bolster our security. For example, Hatcher changed/strengthened passwords, adopted new technical safeguards, provided additional phishing training to employees, and is in the process of building a brand new domain. Hatcher also notified law enforcement.

Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,



Jonathan Wilson
Senior Counsel



THE
HATCHER
AGENCY

The Home of Outrageous Service

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

<<FIRST_NAME>> <<MI>> <<LAST_NAME>>
<<ADDRESS1>>
<<CITY>>, <<state>> <<zip>>

June 16, 2023

Re: Notice of Data Security Incident

Dear <<First_Name>> <<Mi>> <<Last_Name>>::

We are writing to inform you about a data security incident experienced by The Hatcher Agency (“Hatcher”) that may have exposed your personal information to unauthorized persons. We regret that this incident occurred. Although we have no evidence to suggest that any of your personal information has, in fact, been misused, we are providing you with a summary of the incident below and an opportunity to enroll in free credit monitoring and identity left protection services.

WHAT HAPPENED?

On March 14, 2023, Hatcher became aware of some unusual email activity. We immediately began working with cybersecurity experts to investigate and subsequently determined that an unauthorized third party gained access to a portion of Hatcher’s computer network that contained a number of files, including those with personal information. Based on our investigation, we believe the unauthorized access started and ended on February 14, 2023. Once we identified the data that may have been affected, we promptly engaged a data review firm to determine what information was in those files. We received the results of that review in early May. We have been working since then to identify the affected individuals and the correct addresses for them.

WHAT INFORMATION WAS INVOLVED?

Our investigation determined that the following types of personal information related to you may have been impacted: full name, contact information, date of birth, government identification (such as a driver’s license or Social Security number), health insurance information, and a limited amount of medical information.

WHAT WE ARE DOING?

We hired third-party experts to address the situation, investigate the unauthorized activity, and further secure Hatcher’s systems to protect the personal information and data stored on them. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO?

If you have questions about this matter, please call us at the phone number below. Enclosed with this letter you will find additional steps you can take to help protect yourself.

In addition, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/hatcher> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<code>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

FOR MORE INFORMATION:

Hatcher's customers and their personal information is important to us. Should you have any questions, you can contact us at (866) 890-9211, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in black ink, appearing to read "Greg Hatcher", with a stylized, cursive script.

Greg Hatcher, CEO
The Hatcher Agency
310 Louisiana Street
Little Rock, AR 72201

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – Review your account statements and free credit reports.

- 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.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. 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 notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

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

600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

Equifax

P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian

P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion

P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Maryland

Attorney General

200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

New York

Attorney General

The Capitol
Albany, NY 1224
(800) 771-7755
www.ag.ny.gov

North Carolina

Attorney General

9001 Mail Service Center
Raleigh, NC 27699
(919) 716-6400
www.ncdoj.gov

Washington, DC

Attorney General

400 6th St. NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

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

