

October 24, 2022

VIA EMAIL SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: *Notification of Data Security Incident*

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Hartley, Rowe & Fowler P.C. (“Hartley, Rowe & Fowler”), in connection with a recent data security incident that may have affected the information of certain Maryland residents. The purpose of this letter is to notify you of the incident in accordance with Maryland data breach notification statute.

1. Nature of the Security Incident

Hartley, Rowe & Fowler learned of unusual activity involving a Hartley, Rowe & Fowler email account on July 5, 2022 that allowed unauthorized access to the account. Hartley, Rowe & Fowler immediately suspended access to the account and launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. Through its forensic investigation, Hartley, Rowe & Fowler concluded that the email account had been accessed without authorization.

Hartley, Rowe & Fowler also engaged independent experts to conduct a review of data that could have potentially been accessed as a result of the incident, and, on October 4, 2022, determined that the information related to its clients, including the personal information of three Maryland residents. To date, Hartley, Rowe & Fowler has no knowledge that any of this information has been misused.

2. Number of Maryland Residents Involved

Hartley, Rowe & Fowler started notifying the three Maryland residents of this data security incident via first class U.S. mail on October 24, 2022. A sample copy of the notification letter sent to the affected individuals is attached. The information involved differs depending on the individual but may include name, date of birth, phone number, social security number, driver's license or state ID, ID state and account number.

The letter sent to the affected individuals notifying them of the incident offers complimentary identity monitoring services and provides additional steps they can take to protect their personal information.

3. Steps Taken Relating to the Incident

In response to the incident, Hartley, Rowe & Fowler retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise and to prevent similar incidents from occurring in the future. In addition, Hartley, Rowe & Fowler is in the process of reviewing its current security protocols and adding additional security measures.

As discussed above, Hartley, Rowe & Fowler is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

Hartley, Rowe & Fowler is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Jason Cherry at Jason.Cherry@lewisbrisbois.com or (213) 358-6067.

Sincerely,

/s/ Jason Cherry

Jason Cherry of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Individual Notification Letter

Hartley, Rowe & Fowler P.C.
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

HARTLEY, ROWE & FOWLER, P.C.
ATTORNEYS AT LAW

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

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

October 24, 2022

Re: Notice of Data <<Variable>>

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

We are writing to inform you of a data security incident that may have affected some of your personal information. At Hartley, Rowe & Fowler P.C. ("Hartley, Rowe & Fowler"), we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? On July 5, 2022 Hartley, Rowe & Fowler learned of unusual activity involving a Hartley, Rowe & Fowler email account. Upon discovering this activity, we took steps to secure our email environment and launched an investigation with the assistance of a leading independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that a Hartley, Rowe & Fowler email account had been accessed without authorization. Following a comprehensive review of the contents of the email account, we learned on October 4, 2022, that some of your information was contained within. Since that time, we have been gathering current mailing addresses so that we could notify all potentially affected individuals.

What Information Was Involved? The affected information includes your name, address and <<Data Elements>>.

What Are We Doing? As soon as we discovered this 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 are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary credit monitoring and identity protection services for <<12/24 months>> through IDX, a national leader in identity theft protection.

IDX's services include <<12/24 months >> of credit monitoring, CyberScan dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

To help relieve concerns and to help protect your identity following this incident, we are providing you with information about steps you can take to help protect your personal information. Additional information about these steps is included with this letter.

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 U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. You can enroll in the complimentary IDX identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above.

IDX representatives are available Monday through Friday from 9 a.m. to 9 p.m. Eastern Time. Please note the deadline to enroll is January 24, 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 any questions about this letter, please call 1-800-939-4170 Monday through Friday from 9 a.m. to 9 p.m. Eastern Time.

On behalf of Hartley, Rowe & Fowler, thank you for your understanding about this incident. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience this matter may cause you.

Sincerely,

A handwritten signature in cursive script, appearing to read "Robert J. Kauffman".

Robert J. Kauffman, Managing Partner
Hartley, Rowe & Fowler P.C.
Post Office Box 489
Douglasville, Georgia 30133
<<Phone Number>>

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 2000, 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 proof. 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 2000; (202) 727-3400; oag@dc.gov

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>.

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: 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; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, <https://ag.ny.gov/>.

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

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

Washington D.C.: Washington D.C. Attorney General can be reached at: 441 4th Street, NW Washington, DC 20001, 1-202-727-3400, oag.dc.gov.