



LEWIS BRISBOIS BISGAARD & SMITH LLP

Brian Craig  
2112 Pennsylvania Avenue, NW, Suite 500  
Washington DC, 20037  
Brian.Craig@lewisbrisbois.com  
Direct: 202.926.2904

August 12, 2021

**VIA ONLINE PORTAL**

Attorney General Aaron Frey  
Office of the Attorney General  
Consumer Protection Division  
Security Breach Notification  
111 Sewall Street, 6th Floor  
Augusta, ME 04330

**Re: Notification of Data Security Incident**

Dear Attorney General Frey:

We represent Hannis T Bourgeois, LLP (“HTB”), an accounting and business advisor firm with locations throughout Louisiana, in connection with a recent data security incident described below. HTB has notified the impacted individuals of the incident. The purpose of this letter is to provide formal notice to your office.

**I. Nature of the Security Incident**

On January 31, 2021, HTB discovered malicious activity within their environment. Upon learning of this activity, they took steps to secure the digital environment and began an investigation to determine what happened. In so doing, HTB engaged independent cyber experts to determine what happened and whether personal information may have been accessed or acquired without authorization. On May 28, 2021, the investigation determined that personal information in the network could have been accessed or acquired without authorization. The information varies by individual, but may include individuals’ names, dates of birth, driver’s license numbers, passport numbers, Social Security Numbers, financial account numbers, medical diagnosis and treatment information, and payment card number and expiration date and CVV code.

## **II. Number of Maine Residents Affected**

HTB notified eight Maine residents of this data security incident by letters sent via U.S. First Class mail on August 4, 2021 and August 10, 2021. A sample copy of the notification letter sent to the affected individuals is included with this correspondence.

## **III. Actions Taken in Response to the Incident**

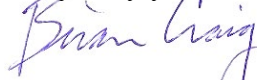
As soon as HTB detected a potential incident, it launched an investigation, engaged a digital forensics firm, and worked to determine whether any personal information was accessed or acquired without authorization. This includes working with leading cybersecurity experts to enhance the security of their digital environment.

HTB also offered identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and Cyberscan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

## **IV. Contact Information**

If you have any questions or need additional information, please do not hesitate to contact me at 202.926.2904 or [Brian.Craig@lewisbrisbois.com](mailto:Brian.Craig@lewisbrisbois.com).

Very truly yours,



Brian Craig of  
LEWIS BRISBOIS BISGAARD & SMITH LLP



P.O. Box 1907  
Suwanee, GA 30024

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

To Enroll, Please Call:  
833-909-3933  
Or Visit:  
<https://response.idx.us/bourgeois>  
Enrollment Code: **XXXXXXXX**

August 4, 2021

Subject: Notice of Data Security Incident:

Dear <<First Name>> <<Last Name>>:

For over 90 years, Hannis T. Bourgeois has worked to exceed the expectations of our clients, our community and each other in all that we do. We are grateful for the trust you have placed in us, and we take the privacy and security of your information very seriously. It is because we value your trust that I am writing to inform you of a data security incident we recently experienced and which may have involved your personal information. Although we have no indication that any of your personal information has been or will be misused, we wanted to ensure that you are aware of the incident and provide you with steps you can take to protect your personal information, should you choose to do so. In addition, as a precautionary measure we are offering you complimentary credit monitoring services for <<Product duration>>.

The incident at issue relates to unusual activity on our computer network discovered on January 31, 2021. As soon as we detected the activity, we immediately contained it and launched an investigation to determine whether any personal information was affected. As part of our investigation, we retained a digital forensics firm, who determined that information in the network could have been accessed or acquired. We reviewed all information and on May 28, 2021 determined that your personal information could have been accessed or acquired in the incident. The information involved includes your name and <<Consolidated Data Elements>>. Again, although we have no indication that any of your personal information has been or will be misused, we are providing you with steps you can take to protect your personal information, including offering you complimentary credit monitoring services for <<Product duration>>.

The following page includes a list of steps you can take to protect your personal information. In addition, you can activate the complimentary credit monitoring services that we are offering for <<Product duration>> through IDX. IDX is a global leader in data security and identity protection, and we specifically selected IDX for their expertise. In order to enroll in the services, please visit <https://response.idx.us/bourgeois> and use the membership number: <<Enrollment Code>>. Please note the deadline to enroll is November 4, 2021. Detailed information about the services are included in the pages that follow.

We know that you may have questions about what happened in the incident, steps you can take to protect your information, and the complimentary services we are offering. In order to better assist you, we have set up a call center to answer your questions. We invite you to call the call center at 833-909-3933 between Monday through Friday from 9 am - 9 pm Eastern Time with any questions you may have. Of course, and as always, we are available and remain ready to serve you at HTB, as well.

Please rest assured that we have implemented enhanced security measures to further safeguard personal information in our possession. These safeguards will help prevent a similar incident from occurring in the future. Please note that the privacy

and security of your personal information is of utmost importance to us. We appreciate your continued trust, and we regret any worry or inconvenience that this incident may cause.

Sincerely,

*Lauren Fitch*

**Lauren M. Fitch**

Director of Operations, Hannis T. Bourgeois, LLP

## 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 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 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:

<b>TransUnion</b> P.O. Box 1000 Chester, PA 19016 1-800-916-8800 <a href="http://www.transunion.com">www.transunion.com</a>	<b>Experian</b> P.O. Box 9701 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>Equifax</b> P.O. Box 740241 Atlanta, GA 30348 866-349-5191 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Free Annual Report</b> P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 <a href="http://annualcreditreport.com">annualcreditreport.com</a>
---	---	--	---

**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 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. 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:** Under U.S. law, 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 at **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, D.C. 20580, or online at [consumer.ftc.gov](http://consumer.ftc.gov) and [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), or to the Attorney General in your state. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

<b>New York Attorney General</b> Bureau of Internet and Technology Resources 28 Liberty Street New York, NY 10005 <a href="mailto:ifraud@ag.ny.gov">ifraud@ag.ny.gov</a> 1-212-416-8433	<b>Maryland Attorney General</b> 200 St. Paul Place Baltimore, MD 21202 <a href="http://oag.state.md.us">oag.state.md.us</a> 410-528-8662	<b>North Carolina Attorney General</b> 9001 Mail Service Center Raleigh, NC 27699 <a href="http://ncdoj.gov">ncdoj.gov</a> 1-877-566-7226	<b>Rhode Island Attorney General</b> 150 South Main Street Providence, RI 02903 <a href="http://www.riag.ri.gov">http://www.riag.ri.gov</a> 401-274-4400
--	---	---	--

**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 others. 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](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).

**Review your Tax Filings:** If you detect any suspicious activity relating to your tax filings, we encourage you to complete IRS Form 14039, Identity Theft Affidavit, which you can obtain at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>. If you have other identity theft / tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490. You should

be especially aware of any requests, calls, emails, letters, or other questions about your financial accounts or from individuals purporting to be from the IRS or other entities from whom you would not be expecting contact. If you receive any type of unexpected request for personal information, you should not provide that information and instead contact the organization by phone to verify the request is legitimate.