

EXHIBIT 1

To the April 25th, 2022 Notice of Data Event

We continue to represent Taylor, Ganson & Perrin, LLP (“TGP”) located at 160 Federal Street, Boston, MA 02110, and write to supplement our February 22, 2022 and March 28, 2022 notices to your office (the “Prior Notices”). The Prior Notices, which contain a full description of this incident, are attached hereto as *Exhibit A*. Through continued efforts to identify potentially affected individuals, TGP identified and provided written notice of this incident to additional individuals on April 25, 2022. TGP reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, TGP does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

On or about April 25, 2022, TGP provided notice of this incident to additional potentially impacted individuals, which includes seventy (70) of Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit B*. The information that could have been subject to unauthorized access or acquisition varies by individual and could include name, and one or more of the following data elements if it was previously provided to TGP: Social Security number, driver’s license number or state identification card number, passport number, military identification number, financial account information, credit card number, medical information, health insurance information, username and password for online accounts, digital signature and/or taxpayer identification number.

Upon discovering the event, TGP investigated and responded to the incident, assessed the security of TGP systems, and notified potentially affected individuals. In order to promptly alert potentially impacted individuals, TGP provided substitute notice while continuing to work to determine whether it could identify the individual notice population. Upon identification of the potentially impacted population, TGP moved quickly to provide written notice of this incident to individuals and to supplement notice to regulators. TGP is also working to implement additional safeguards and training to its employees. TGP is providing access to credit monitoring services for 2 years through IDX to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TGP is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TGP is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

To the April 25th, 2022 Notice of Data Event

Maine Security Breach Reporting Form

Thank you for submitting the breach details through this reporting form. The information you have provided has been submitted to the agency.

Please close this browser window.

< PREVIOUS

FINISH

© Copyright 2022, NIC, Inc.

Maine Security Breach Reporting Form - Review

[EDIT](#)

Type of Organization (Please select one)	Other Commercial
Entity Name	Taylor, Ganson & Perrin, LLP
Street Address	160 Federal Street
City	Boston
State, or Country if outside the US	MA
Zip Code	02110
Name	John Fulginiti
Title	Partner
Telephone Number	(617) 951-2777
Email Address	jfulginiti@taylorganson.com
Relationship to entity whose information was compromised	Partner
Total number of persons affected (including Maine residents)	6317
Total number of Maine residents affected	75
If the number of Maine residents exceeds 1,000, have the consumer reporting agencies been notified?	No

Date(s) Breach Occurred	12/14/2021
Date Breach Discovered	01/27/2022
Description of the Breach (please check all that apply)	External system breach (hacking)
Information Acquired - Name or other personal identifier in combination with (please check all that apply)	Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account) Driver's License Number or Non-Driver Identification Card Number Social Security Number
Type of notification	Written
Date(s) of consumer notification	03/28/22
List dates of any previous (within 12 months) breach notifications	Substitute Notice - 02/22/2022
Were identity theft protection services offered?	Yes
If yes, please provide the duration, the provider of the service and a brief description of the service	24 months; IDX; Credit monitoring and identity restoration services.

[< PREVIOUS](#)
[CONTINUE TO SUBMIT FORM >](#)

EXHIBIT 1

We write to supplement our February 22, 2022 notice to your office (the “February 22nd Notice”). The February 22nd Notice, which contains a full description of this incident, is attached hereto as **Exhibit A**. At the time of the February 22nd Notice, TGP provided substitute notice to potentially impacted individuals through website and media notice. Based upon ongoing efforts to accurately identify the potentially affected individuals, TGP began providing written notice of this incident to individuals on March 28, 2022. TGP reserves the right to supplement this notice with any new significant facts learned subsequent to its submission. By providing this notice, TGP does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

On or about March 28, 2022, TGP provided written notice of this incident to potentially impacted individuals, which includes seventy-five (75) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit B**. The information that could have been subject to unauthorized access or acquisition varies by individual and could include name, and one or more of the following data elements if it was previously provided to TGP: Social Security number, driver’s license number or state identification card number, passport number, military identification number, financial account information, credit card number, medical information, health insurance information, username and password for online accounts, digital signature and/or taxpayer identification number.

Upon discovering the event, TGP moved quickly to investigate and respond to the incident, assess the security of TGP systems, and notify potentially affected individuals. In order to promptly alert potentially impacted individuals, TGP provided substitute notice while continuing to work to determine whether it could identify the individual notice population. Upon identification of the potentially impacted population, TGP moved quickly to provide written notice of this incident to individuals and to supplement notice to regulators. TGP is also working to implement additional safeguards and training to its employees. TGP is providing access to credit monitoring services for two (2) years through IDX to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TGP is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TGP is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Kevin M. Mekler
Office: (267) 930-2190
Fax: (267) 930-4771
Email: Kmekler@mullen.law

3001 N. Rocky Point Drive East, Suite 200
Tampa, FL 33607

February 22, 2022

VIA E-MAIL:

Office of the Maine Attorney General
Security Breach Notification
Consumer Protection Division
111 Sewall Street, 6th Floor
Augusta, ME 04330
E-mail: breach.security@maine.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Taylor, Ganson & Perrin, LLP (“TGP”) located at 160 Federal Street, Boston, MA 02110, and are writing to notify your office of an incident that may affect the security of some personal information relating to an unknown number of Maine residents. While we are aware that Maine provides an online form for reporting incidents, we are submitting this notice via written letter as TGP cannot provide certain information required for the form submission at this time, including total number of state residents impacted. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TGP does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about January 23, 2022, TGP discovered unusual activity on certain computer systems. TGP quickly disconnected these systems from the network and commenced an intensive investigation to determine the source and scope of the incident. Although the investigation is not complete at this time, on or about January 27, 2022, the investigation determined that certain information stored within the TGP environment had been accessed and/or acquired by an unauthorized actor in connection with this incident. At this stage in the investigation, TGP is unable to provide an estimated number of impacted individuals. TGP continues to investigate the scope of the unauthorized access to determine what specific information may have been accessed and/or acquired and to whom that information relates.

The information that could have been subject to unauthorized access includes name, Social Security number, driver's license number or state identification card number, financial account information, credit card number and/or username and password for online accounts.

Notice to Maine Residents

On or about February 22, 2022, TGP provided substitute notice of this incident to potentially impacted, which includes publication of this incident on TGP's website and media notice. Substitute notice is being provided in substantially the same form as the website and media notices attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, TGP moved quickly to investigate and respond to the incident, assess the security of TGP systems, and notify potentially affected individuals. In order to promptly alert potentially impacted individuals, TGP provided substitute notice while continuing to work to determine whether it can identify the individual notice population. If so, TGP will provide written notice to the impacted population upon identification of the appropriate individuals. TGP is also working to implement additional safeguards and training to its employees. TGP is providing access to credit monitoring services for two (2) years, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, TGP is providing impacted individuals with guidance on how to better protect against identity theft and fraud. TGP is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2190.

Very truly yours,



Kevin M. Mekler of
MULLEN COUGHLIN LLC

EXHIBIT A

To the February 22, 2022 Notice of Data Event

Taylor, Ganson & Perrin LLP Provides Notice of Data Privacy Event

Boston, MA – February 22, 2022 – Taylor, Ganson & Perrin LLP (“TGP”) is providing notice of a recent event that may affect the privacy of certain personal information. TGP provides legal services to individuals, families, trusts and businesses primarily throughout Massachusetts. Information about TGP can be found at <http://www.taylorganson.com/>. TGP is providing information about this event, TGP’s response to it, and resources available to individuals to help protect their information, should they feel it necessary to do so.

What Happened? On January 23, 2022, TGP discovered unusual activity on certain computer systems. TGP quickly disconnected these systems from the network and commenced an intensive investigation to determine the source and scope of the incident. Although the investigation is not complete at this time, on or about January 27, 2022, the investigation determined that certain information stored within the TGP environment had been accessed and/or acquired by an unauthorized actor in connection with this incident. However, TGP continues to investigate the scope of the unauthorized access to determine what specific information may have been accessed and/or acquired and to whom that information relates. TGP is providing this notice in an abundance of caution to inform you of the incident so that you may take steps to protect your information.

What Information Was Involved? The information that may have been subject to access and/or exfiltration varies by individual based upon the information provided to TGP. The type of information could include name, Social Security number, driver’s license number or state identification card number, passport number, military identification number, financial account information, credit card number, medical information, health insurance information, username and password for online accounts, digital signature and/or taxpayer identification number.

How Will Individuals Know If They Are Affected By This Incident? If you would like to know if you are potentially affected by this incident, please call TGP’s dedicated assistance line, detailed below.

What We Are Doing. TGP takes this incident very seriously. Information privacy and security are among TGP’s highest priorities, and TGP has strict security measures in place to protect information in its care. Upon discovering this incident, TGP quickly took steps to investigate and respond, including reporting this incident to federal law enforcement and notifying potentially affected individuals and relevant regulators. Moreover, as an added precaution, TGP is offering complimentary access to credit monitoring and identity restoration services to potentially impacted individuals through IDX.

What You Can Do. TGP encourages you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. As an added precaution, TGP is offering potentially impacted individuals access to 24 months of free credit monitoring and identity restoration services through IDX. To enroll in the complimentary credit monitoring services, please call our dedicated assistance line at 1-833-783-1439.

Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before

extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax, P.O. Box 105069, Atlanta, GA, 30348, 1-800-685-1111, www.equifax.com; **Experian**, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; **TransUnion**, P.O. Box 2000, Chester, PA 19016, 800-680-7289, www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement or the individual’s state Attorney General.

TGP wants to assure those who may be impacted that TGP takes the responsibility to safeguard personal information very seriously. TGP deeply regrets any inconvenience or concern this incident may cause you. If you have additional questions, please call our dedicated assistance line at 1-833-783-1439 (toll free), Monday through Friday, from 9 am - 9 pm Eastern Time (excluding U.S. holidays).

Notice of Data Privacy Event

Taylor, Ganson & Perrin LLP (“TGP”) is providing notice of a recent event that may affect the privacy of certain personal information. TGP is providing information about this event, TGP’s response to it, and resources available to individuals to help protect their information, should they feel it necessary to do so.

What Happened? On January 23, 2022, TGP discovered unusual activity on certain computer systems. TGP quickly disconnected these systems from the network and commenced an intensive investigation to determine the source and scope of the incident. Although the investigation is not complete at this time, on or about January 27, 2022, the investigation determined that certain information stored within the TGP environment had been accessed and/or acquired by an unauthorized actor in connection with this incident. TGP continues to investigate the scope of the unauthorized access to determine what specific information may have been accessed and/or acquired and to whom that information relates. However, we are providing this notice in an abundance of caution to inform you of the incident so that you may take steps to protect your information.

What Information Was Involved? The information that may have been subject to access and/or exfiltration varies by individual based upon the information provided to TGP. The type of information could include name, Social Security number, driver’s license number or state identification card number, passport number, military identification number, financial account information, credit card number, medical information, health insurance information, username and password for online accounts, digital signature and/or taxpayer identification number.

How Will Individuals Know If They Are Affected By This Incident? If you would like to know if you are potentially affected by this incident, please call TGP’s dedicated assistance line, detailed below.

What We Are Doing. We take this incident very seriously. Information privacy and security are among our highest priorities, and we have strict security measures in place to protect information in our care. Upon discovering this incident, we quickly took steps to investigate and respond, including reporting this incident to federal law enforcement and notifying potentially affected individuals and relevant regulators. Moreover, as an added precaution, TGP is offering complimentary access to credit monitoring and identity restoration services to potentially impacted individuals through IDX.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. As an added precaution, we are offering potentially impacted individuals access to 24 months of free credit monitoring and identity restoration services through IDX. To enroll in the complimentary credit monitoring services, please call our dedicated assistance line at 1-833-783-1439.

Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax, P.O. Box 105069, Atlanta, GA, 30348, 1-800-685-1111, www.equifax.com; **Experian**, P.O. Box 2002, Allen, TX 75013, 888-397-3742, www.experian.com; **TransUnion**, P.O. Box 2000, Chester, PA 19016, 800-680-7289, www.transunion.com. Potentially impacted individuals may also find information regarding identity theft, fraud alerts, security freezes and the steps they may take to protect their information by contacting the credit bureaus, the Federal Trade Commission or their state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should also be reported to law enforcement or the individual’s state Attorney General.

TGP wants to assure those who may be impacted that we take the responsibility to safeguard personal information very seriously. We deeply regrets any inconvenience or concern this incident may cause you. If you have additional questions, please call our dedicated assistance line at 1-833-783-1439 (toll free), Monday through Friday, from 9 am - 9 pm Eastern Time (excluding U.S. holidays).

EXHIBIT B

Taylor, Ganson & Perrin, LLP
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call: 1-833-783-1439 Or Visit: https://response.idx.us/taylorganson Enrollment Code: [XXXXXXXXXX]
--

<<First Name>> <<Last Name>>
<<Care of>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

March 28, 2022

NOTICE OF <<VARIABLE 1>>

Dear <<Fist Name>> <<Last Name>>:

The purpose of this letter is to notify you about a recent data incident that may involve some of your information. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so.

What Happened? On January 23, 2022, Taylor, Ganson & Perrin, LLP (“TGP”) discovered unusual activity on certain computer systems. TGP quickly disconnected these systems from the network and commenced an intensive investigation to determine the source and scope of the incident. On or about January 27, 2022, the investigation determined that certain information stored within the TGP environment was potentially accessed and/or acquired by an unauthorized actor in connection with this incident. Thereafter, TGP provided substitute notice of this incident on February 22, 2022, and continued to investigate the scope of the unauthorized access to determine what specific information may have been accessed and/or acquired and to whom that information relates. On March 14, 2022, TGP was able to compile a list of individuals whose information resided on the impacted systems, including address information sufficient to permit individual notice. We are providing this notice in an abundance of caution to inform you of the incident so that you may take steps to protect your information.

What Information Was Involved? The information that was potentially subject to access and/or exfiltration could include your name and one or more of the following data elements if it was previously provided to TGP: Social Security number, driver’s license number or state identification card number, passport number, military identification number, financial account information, credit card number, medical information, health insurance information, username and password for online accounts, digital signature and/or taxpayer identification number.

What We Are Doing. We take this incident very seriously. Information privacy and security are among our highest priorities, and we have strict security measures in place to protect information in our care. Upon discovering this incident, we quickly took steps to investigate and respond, including reporting this incident to federal law enforcement and notifying potentially affected individuals and relevant regulators. Moreover, as an added precaution, TGP is offering complimentary access to credit monitoring and identity restoration services to potentially impacted individuals through IDX.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. As an added precaution, we are offering you access to 24 months of free credit/identity monitoring and identity restoration services through IDX. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Steps You Can Take to Help Protect Personal Information*.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-833-783-1439 (toll free), Monday through Friday, from 9 am - 9 pm Eastern Time (excluding U.S. holidays). You may write to TGP at 160 Federal Street, 20th Floor, Boston, MA 02110.

Sincerely,

Taylor, Ganson & Perrin, LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

1. Website and Enrollment. Go to <https://response.idx.us/taylorjanson> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is June 28, 2022.
2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. Telephone. Contact IDX at 1-833-783-1439 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<#>> Rhode Island residents impacted by this incident.

EXHIBIT B

To the April 25th, 2022 Notice of Data Event

Taylor, Ganson & Perrin, LLP
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call: 1-833-783-1439 Or Visit: https://response.idx.us/taylorganson Enrollment Code: [XXXXXXXXXX]
--

<<First Name>> <<Last Name>>
<<Address 1>> <<Address 2>>
<<City>>, <<State>> <<Zip>>

April 25, 2022

NOTICE OF <<VARIABLE 1>>

Dear <<Fist Name>> <<Last Name>>:

The purpose of this letter is to notify you about a recent data incident that may involve some of your information. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so.

What Happened? On January 23, 2022, Taylor, Ganson & Perrin, LLP (“TGP”) discovered unusual activity on certain computer systems. TGP quickly disconnected these systems from the network and commenced an intensive investigation to determine the source and scope of the incident. On or about January 27, 2022, the investigation determined that certain information stored within the TGP environment was potentially accessed and/or acquired by an unauthorized actor in connection with this incident. Thereafter, TGP provided substitute notice of this incident on February 22, 2022, and continued to investigate the scope of the unauthorized access to determine what specific information may have been accessed and/or acquired and to whom that information relates. On April 8, 2022, TGP was able to compile a list of individuals whose information resided on the impacted systems, including address information sufficient to permit individual notice. We are providing this notice in an abundance of caution to inform you of the incident so that you may take steps to protect your information.

What Information Was Involved? The information that was potentially subject to access and/or exfiltration could include your name and one or more of the following data elements if it was previously provided to TGP: Social Security number, driver’s license number or state identification card number, passport number, military identification number, financial account information, credit card number, medical information, health insurance information, username and password for online accounts, digital signature and/or taxpayer identification number.

What We Are Doing. We take this incident very seriously. Information privacy and security are among our highest priorities, and we have strict security measures in place to protect information in our care. Upon discovering this incident, we quickly took steps to investigate and respond, including reporting this incident to federal law enforcement and notifying potentially affected individuals and relevant regulators. Moreover, as an added precaution, TGP is offering complimentary access to credit monitoring and identity restoration services to potentially impacted individuals through IDX.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. As an added precaution, we are offering you access to 24 months of free credit/identity monitoring and identity restoration services through IDX. Instructions for enrolling in the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached *Steps You Can Take to Help Protect Personal Information*.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-833-783-1439 (toll free), Monday through Friday, from 9 am - 9 pm Eastern Time (excluding U.S. holidays). You may write to TGP at 160 Federal Street, 20th Floor, Boston, MA 02110.

Sincerely,

Taylor, Ganson & Perrin, LLP

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

1. Website and Enrollment. Go to <https://response.idx.us/taylorjanson> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is June 28, 2022.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-783-1439 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are <<Number of RI>> Rhode Island residents impacted by this incident.