

RECEIVED

NOV 24 2020

CONSUMER PROTECTION



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 16, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Gibbs & Cox, Inc. ("Gibbs & Cox"), located at 2711 Richmond Highway, Suite 1000, Arlington, VA 22202 and are writing to notify your office of an incident that may affect the security of personal information relating to approximately three (3) New Hampshire residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Gibbs & Cox does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

In October of 2019, Gibbs & Cox learned of suspicious activity occurring within certain company computer systems. Gibbs & Cox immediately launched an investigation in cooperation with federal law enforcement. This extensive investigation included the assistance of third-party computer forensic specialists, who worked to determine the nature and scope of the incident. The investigation indicated certain Gibbs & Cox systems were accessible for various periods of time by an unknown actor between March 2017 and December 2019, and limited data, which may have contained personal information, was taken by the unknown actor. In an abundance of caution, Gibbs & Cox began working with specialists to conduct a comprehensive review of the information taken by the unknown actor to identify the individuals whose information may have been impacted. On or about October 8, 2020, Gibbs & Cox confirmed the identities and contact information of the individuals who may have had information affected by this incident.

Mullen.law

Although the types of personal information potentially impacted varies by individual, the types of personal information affected for New Hampshire residents includes: name, address, and telephone number, social security number, email address, birth date and birth place, gender, race, military status, bank information (for direct deposit), driver's license number, and passport information (number, issue date, expiration date) .

Notice to New Hampshire Residents

On November 16, 2020, Gibbs & Cox began providing written notice of this incident to individuals who were affected, which includes approximately three (3) New Hampshire residents. Written notice was provided to affected individuals in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Gibbs & Cox moved quickly to investigate the event in cooperation with federal law enforcement, identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. Gibbs & Cox also implemented additional industry-leading safeguards to protect the security of information in its systems. Gibbs & Cox also notified other government regulators.

Gibbs & Cox is providing written notice to those individuals who may be affected by this incident. This notice includes an offer of complimentary access to 24 months of credit monitoring and identity restoration services through TransUnion, and the contact information for a dedicated assistance line for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Gibbs & Cox is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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.

Office of the New Hampshire Attorney General
November 16, 2020
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,

Sian M. Schafle

Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS:szs
Enclosure

STATE OF NH
DEPT OF JUSTICE
2020 NOV 24 AM 11:22

EXHIBIT A



Return Mail Processing Center
PO Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Gibbs & Cox, Inc. (“Gibbs & Cox”), is writing to inform you of an event that may impact the security of some of your personal information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? In October of 2019, Gibbs & Cox learned of suspicious activity occurring within certain company computer systems. Gibbs & Cox immediately launched an investigation in cooperation with federal law enforcement. This extensive investigation included the assistance of third-party computer forensic specialists, who worked to determine the nature and scope of the incident. The investigation indicated certain Gibbs & Cox systems were accessible for various periods of time by an unknown actor between March 2017 and December 2019, and limited data, which may have included personal information, was taken by the unknown actor. In an abundance of caution, Gibbs & Cox began working with specialists to conduct a comprehensive review of the information taken by the unknown actor to identify the individuals whose information may have been impacted. Gibbs & Cox recently completed its internal review to determine the identities and contact information for potentially impacted individuals.

What Information Was Involved. We recently determined the following types of information relating to you may have been present in Gibbs & Cox’s systems at the time of the incident: name, address, telephone number, Social Security number, email address, birth date, gender, race, military status, bank information (for direct deposit), driver’s license number and passport information (number, issue date, expiration date). We have not received any reports of actual misuse of your information, and we are providing this notification in an abundance of caution.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took substantial steps to further secure our systems. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional safeguards to further secure the information in our systems. Gibbs & Cox has also worked closely with federal law enforcement and other government agencies and regulators. Although we have no indication of actual misuse of your information, we are offering you access to 24 months of credit monitoring and identity restoration services through TransUnion.

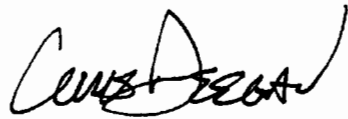
What You Can Do. You can find out more about how to better protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank and credit card account statements, and to monitor your credit reports for suspicious activity. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 855-914-4681, Monday through Friday (excluding U.S. holidays), during the hours of 9:00 a.m. to 9:00 p.m., Eastern Time (excluding U.S. holidays). You may also write to Gibbs & Cox at 2711 Richmond Highway, Suite 1000 Arlington, VA 22202.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

GIBBS & COX, INC.

A handwritten signature in black ink, appearing to read "CHRIS DEEGAN". The signature is stylized and cursive.

CHRIS DEEGAN
President & Chief Executive

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enrollment Instructions

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<6 Digit Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior 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.);

7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
[www.transunion.com/
fraud-victim-resource/
place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your 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. 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 Maryland residents: The Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662; and www.oag.state.md.us.

For North Carolina residents: The 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. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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 agencies 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 Rhode Island residents: The Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 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 7 Rhode Island residents impacted by this incident.

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

For Washington, D.C. residents: The Attorney General may be contacted at: Office of the Attorney General, 441 4th Street, NW, Washington, DC 20001; (202) 727-3400; and www.oag@dc.gov.