



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

JUL 12 2021

CONSUMER PROTECTION

Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

4843 Colleyville Blvd, Suite 251-388
Colleyville, TX 76034

July 9, 2021

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 Hughes Socol Piers Resnick & Dym, Ltd. ("HSPRD"), located at 70 W. Madison Street, Suite 4000, Chicago, Illinois 60602, and are writing to notify your Office of an incident that may affect the security of some personal information relating to four (4) New Hampshire residents. 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, HSPRD does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 13, 2020, certain HSPRD systems became infected with a virus that prohibited access to certain files and systems. Upon discovery, HSPRD immediately commenced an investigation, which included working with third-party IT and forensic investigators, to determine the full nature and scope of the incident and to secure our network. Through this investigation, HSPRD determined that an unauthorized actor had placed malware within their environment that disrupted the operation of certain HSPRD systems. On or about September 28, 2020, HSPRD's investigation further determined that the unauthorized actor had gained access to certain HSPRD systems between August 28, 2020 and September 14, 2020. As a result, the unauthorized actor may have had access to certain files within these systems.

HSPRD performed an extensive investigation to determine what, if any, sensitive data was potentially involved. This investigation included working diligently to gather further information to understand the scope of the incident. For the past several months, HSPRD sent notices to the known impacted population. On May 18, 2021, HSPRD completed its data review, and unfortunately, located additional individuals potentially affected by this incident. HSPRD is now taking steps to notify those additional individuals.

Mullen.law

Notice to New Hampshire Residents

On or about November 10, 2020, HSPRD began providing written notice of this incident to affected individuals. On July 9, 2021, HSPRD is providing notice to the additionally identified individuals, which includes four (4) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken


Upon discovering the event, HSPRD moved quickly to investigate and respond to the incident, assess the security of HSPRD systems, and notify potentially affected individuals and HSPRD clients. HSPRD is also working to implement additional safeguards and training to its employees. While HSPRD is not aware of any actual or attempted misuse of this information, HSPRD is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, HSPRD is providing 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1697.

Very truly yours,

A handwritten signature in black ink, appearing to read "Amanda Harvey". The signature is fluid and cursive, with a long horizontal stroke at the end.

Amanda Harvey of
MULLEN COUGHLIN LLC

ANH/eeb
Enclosure

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

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

Re: Notice of Data Breach

Dear <<Name 1>>:

Hughes Socol Piers Resnick & Dym, Ltd. ("HSPRD") writes to inform you of a recent incident that may affect the security of some of your information related to HSPRD's representation of you. While we are unaware of any actual or attempted misuse of your personal information, we are providing you with an overview of the incident, our response, and steps you may take to better protect yourself, should you feel it necessary to do so.

What Happened? On September 13, 2020, certain HSPRD systems became infected with a virus that prohibited access to certain files and systems. Upon discovery, HSPRD immediately commenced an investigation, which included working with third-party IT and forensic investigators, to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that an unauthorized actor had placed malware within our environment that disrupted the operation of certain HSPRD systems. On or about September 28, 2020, HSPRD's investigation further determined that the unauthorized actor had gained access to certain HSPRD systems between August 28, 2020 and September 14, 2020. As a result, the unauthorized actor may have had access to certain files within these systems.

HSPRD performed an extensive investigation to determine what, if any, sensitive data was potentially involved. This investigation included working diligently to gather further information to understand the scope of the incident. For the past several months, HSPRD sent notices to the known impacted population. On May 18, 2021, HSPRD completed its data mining, and unfortunately, located additional individuals potentially affected by this incident. As such, you are receiving this letter.

What Information Was Involved? While the investigation was able to determine that these systems were accessed, HSPRD was unable to determine all of the sensitive information that was actually accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, HSPRD conducted a review of the affected systems and is notifying you of this incident because the following types of information related to you may have been present at the time of the incident: <<Data Elements>>. To date, HSPRD has not received any reports of actual or attempted misuse of your information.

What Are We Doing? The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. When we discovered this incident, we immediately launched an investigation and took steps to secure our systems and determine what personal, confidential, and client data might be at risk. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security. We will also be notifying state and federal regulators, as required.

As an added precaution, we are also offering you complimentary access to one year of credit monitoring and identity theft restoration services through TransUnion. We encourage you to activate these services, as we are not able to act on your behalf to activate them for you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Can You Do? We encourage you to review the enclosed *Steps You Can Take To Help Protect Your Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also activate the complimentary credit and identity monitoring services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-914-4642 between the hours of 9am to 9pm, Monday through Friday, excluding major U.S. holidays. You may also write to HSPRD at 70 W. Madison Street, Suite 4000, Chicago, Illinois 60602.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Christopher J. Wilmes
Hughes Socol Piers Resnick & Dym, Ltd.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit and Identity Monitoring

Complimentary One-Year myTrueIdentity Credit Monitoring Service

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

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the myTrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 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 six-digit telephone passcode <<Insert static 6-digit Telephone 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. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year 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, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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 fraud alert or 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 HYPERLINK "<mailto:oag@dc.gov>" 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 HYPERLINK "<http://www.oag.state.md.us>" www.oag.state.md.us. Lucky is located at 555 E. North Lane, Suite 6050, Conshohocken, PA 19428.

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 HYPERLINK "<http://www.ncdoj.gov>" www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; HYPERLINK "<http://www.riag.ri.gov>" 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.

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 HYPERLINK "http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra" 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 HYPERLINK "<https://ag.ny.gov>" <https://ag.ny.gov>.