



**MULLEN  
COUGHLIN**<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED  
MAR 15 2021  
CONSUMER PROTECTION

Christopher J. DiIenno  
Office: (267) 930-4775  
Fax: (267) 930-4771  
Email: [cdiienna@mullen.law](mailto:cdiienna@mullen.law)

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

March 3, 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 Sachs Sax Caplan P.L. ("SSC") located at 6111 Broken Sound Parkway NW, Suite 200 Boca Raton, FL 33487, 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. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SSC 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 February 26, 2020, SSC identified suspicious activity related to certain SSC systems. Upon discovery, SSC immediately commenced an investigation, which included working with third-party forensic specialists, to determine the full nature and scope of the incident and to secure its network. SSC determined that an unauthorized actor gained access to certain systems and email accounts within its environment in January and February 2020. As a result, the unauthorized actor may have gained access to or exfiltrated information located within these systems and email accounts. While SSC was able to determine that these systems and email accounts were accessed, SSC was unable to determine which sensitive information located within these systems and email accounts may have been actually accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, SSC conducted an extensive programmatic and manual review of the affected systems and email accounts to identify all of the information stored therein that may have been affected by this event.

The information that could have been subject to unauthorized access or acquisition includes name and one or more of the following types of information: financial account number, driver's license or state identification card number, and Social Security number.

### **Notice to New Hampshire Residents**

On March 2, 2021, SSC provided written notice of this incident to all affected individuals, which includes approximately 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**

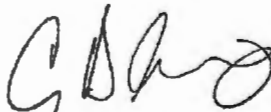
Upon discovering the event, SSC moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. SSC is also working to implement additional safeguards and training to its employees. SSC is providing access to credit monitoring services for one (1) year through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SSC is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. SSC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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) 930-4775.

Very truly yours,



Christopher J. DiLenno of  
MULLEN COUGHLIN LLC

# 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>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>> <<Date>>

**Re: Notice of Data <<Variable Header>>**

Dear <<Name 1>>:

Sachs Sax Caplan, P.L. ("SSC") writes to inform you of an incident that may affect the security of some of your information. SSC received your information in connection with a legal matter in which you, or someone related to you, were involved. 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 wish to do so.

**What Happened?** On February 26, 2020, SSC identified suspicious activity related to certain SSC systems. Upon discovery, SSC immediately commenced an investigation, which included working with third-party 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 gained access to certain systems and email accounts within the SSC environment in January and February 2020. As a result, the unauthorized actor may have gained access to or exfiltrated information located within these systems and email accounts.

**What Information Was Involved?** While the investigation was able to determine that these systems and email accounts were accessed, SSC was unable to determine which sensitive information located within these systems and email accounts was actually accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, SSC, with the assistance of third-party forensic investigators, conducted an extensive programmatic and manual review of the affected systems and email accounts. SSC is notifying you of this incident because our review confirmed your information was present in the affected systems or email accounts. This information included your name and <<Breached Elements>>. To date, SSC has not received any reports of actual or attempted misuse of your information.

**What We Are 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 have reviewed our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security, including safeguards at our outside IT service providers. We will also be notifying state and federal regulators, as required.

As an added precaution, we are also offering you complimentary access to <<Variable Data>> months 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 You Can 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 800-668-0605 between the hours of 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays. You may also write to SSC at 6111 Broken Sound Pkwy NW #200, Boca Raton, FL 33487.

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

Sincerely,

A handwritten signature in black ink that reads "Spencer Sax". The signature is written in a cursive, flowing style.

Spencer Sax, Managing Partner  
Sachs Sax Caplan, P.L.

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### **Enroll in Credit and Identity Monitoring**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<Variable Data>> months provided by TransUnion Interactive, a subsidiary of TransUnion,<sup>®</sup> 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](http://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 COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain unlimited access to your TransUnion credit report and credit score for the duration of the monitoring service.
- 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 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](http://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](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://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](http://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, provide 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, include 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](http://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](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); 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 can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, [www.oag.state.md.us](http://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 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 a 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](http://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 North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**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; <http://ag.ny.gov/>.

**For Rhode Island residents**, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; [www.riag.ri.gov](http://www.riag.ri.gov), 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 approximately 2 Rhode Island residents impacted by this incident.

**For Washington, D.C. residents**, the Office of Attorney General for the District of Columbia can be reached at: 441 4<sup>th</sup> Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; [https://oag.dc.gov](http://oag.dc.gov).