WINSTON & STRAWN LLP

North America Europe Asia

35 W. Wacker Drive
Chicago, IL 60601
T +1 312 558 5600
F +1 312 558 5700

ALESSANDRA V. SWANSON
Partner
(312) 558-7435
ASwanson@winston.com

VIA OVERNIGHT MAIL

August 24, 2020

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Privacy Incident

Attorney General MacDonald:

Winston & Strawn LLP ("Winston") represents Schramm, Inc. ("Schramm") with respect to the privacy incident that is the subject of this letter. I am writing to inform your office of the incident pursuant to New Hampshire law, as the incident affected one (1) New Hampshire resident.

Schramm's business address is 800 E. Virginia Avenue, West Chester, Pennsylvania, 19380. Schramm recently experienced a privacy incident that potentially affected personal information stored on its information systems. Namely, on July 10, 2020, Schramm became aware of suspicious activity on its information systems. Schramm immediately launched an investigation, which included working with information security and forensics experts. Through this assessment, Schramm determined that an unauthorized actor gained access to its information systems on or around June 26, 2020. Schramm was able to restore the operability of, and remove the unauthorized actor's access to, its systems shortly thereafter. Schramm's investigation also revealed that the unauthorized third party obtained a copy of several data files from its information systems before the vulnerability was remediated.

Upon learning of this incident, Schramm immediately took steps to confirm the security of its systems, including by resetting passwords for affected systems, implementing increased security measures for administrative account and server access, and reviewing its company procedures relating to data security. Schramm also notified, and cooperated with, law enforcement. Schramm is working with an information security vendor to determine how it can learn from this event to best avoid similar incidents in the future.

In connection with its ongoing investigation, on July 29, 2020, Schramm determined that personal information, including the name, contact information and Social Security number of one New Hampshire resident, may have been impacted by this incident.

Out of an abundance of caution, beginning as of the date of this letter, Schramm is providing affected individuals with notification of the incident, along with information regarding steps they may take to further protect themselves from fraud and identity theft. A sample notification letter is enclosed for your office's reference. In addition, Schramm has contracted with ID Experts to provide two years of membership in the MyIDCare service at no cost to all confirmed affected individuals. Per ID Experts, as part of the MyIDCare membership, such individuals will receive services including two years of credit monitoring. Schramm anticipates concluding the notification process on or around August 26, 2020.

Please note that, by providing this information, Schramm expressly reserves all available rights, defenses, and privileges in connection with this incident. Furthermore, Schramm does not admit or concede any liability or wrongdoing, and expressly reserves its right to contest or challenge any findings or conclusions of the any investigation by this office or any other office or agency with appropriate jurisdiction. Finally, this notice is not, and does not otherwise constitute, a waiver of Schramm's objection that New Hampshire lacks personal jurisdiction with respect to the incident.

It is my hope that this information will satisfy this office's need for information related to this incident. However, if this office requires any additional details, please contact me by telephone at (312) 558-7435 or via email at ASwanson@winston.com.

Sincerely,

Alessandra V. Swanson

Enclosure: Sample Notification Letter

Schramm, Inc.
C/O ID Experts
10300 SW Greenburg Rd, Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

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

August 24, 2020

Dear <<First Name>> <<Last Name>>,

Schramm, Inc. ("Schramm") is writing to notify you of an event that may affect the security of some of your personal information. This letter provides details of the incident, our response, and resources available to you. We are providing this notice out of an abundance of caution so that you may take action to protect your personal information if you feel it is appropriate to do so.

What Happened? On July 10, 2020, Schramm became aware of suspicious activity on our information systems. We immediately launched an investigation, which included working with information security and forensics experts. Through this assessment, we determined that an unauthorized actor gained access to our information systems on or around June 26, 2020. We were able to restore the operability of, and remove the unauthorized actor's access to, our systems shortly thereafter. Our investigation also revealed that the unauthorized third party obtained a copy of several data files from our information systems before the vulnerability was remediated.

What Information Was Involved? In connection with our ongoing investigation, on July 29, 2020, we determined that some of your personal information may have been impacted by this incident. Out of an abundance of caution, we wanted to let you know that this may have included your first and last name, contact information (e.g., your address) and your Social Security number.

What Are We Doing. Information privacy and security are among our highest priorities. Upon learning of this incident, we immediately took steps to confirm the security of our systems. We reset passwords for affected systems, implemented increased security measures for administrative account and server access, and reviewed our company procedures relating to data security. We also notified, and cooperated with, law enforcement. We are working with an information security vendor to determine how we can learn from this event to best avoid similar incidents in the future. In addition, we are notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so.

We are offering you, at no cost, MyIDCare™ identity theft protection services through ID Experts®. MyIDCare services include 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What Can You Do. You may review the information contained in the attached "Recommended Steps to Help Protect Your Information." You may also enroll to receive the identity theft protection services we are making available to you. Schramm will cover the cost of this service; however, you will need to enroll yourself in this service by November 24, 2020. Please call 1-800-939-4170 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

How To Get More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-800-939-4170 (toll free), Monday through Friday, 8:00 a.m. to 8:00 p.m., CST.

A Special Note About Minors. If this letter relates to a minor child, we recommend that the child's parent or guardian call the dedicated assistance line to enroll the child in MyIDCare or to obtain more information about the incident.

We sincerely regret any inconvenience this incident may cause you.

Sincerely,

[redacted]

Schramm, Inc.

MyIDCare

Recommended Steps to Help Protect Your Information

1. Enroll in MyIDCare. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare 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, MyIDCare will be able to assist you.

3. Call for more information. Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with 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.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team, who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place fraud alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-800-525-6285	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Request a security freeze. By placing a security freeze, someone who fraudulently acquires your personal information will not be able to use that personal information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. **Obtain additional information about the steps you can take to avoid identity theft.** You can request this information from the agencies listed below. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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. You can 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.

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; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.