MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Gregory Bautista
Office: (267) 930-1509
Fax: (267) 930-4771
Email: gbautista@mullen.law

1127 High Ridge Road, #301
Stamford, CT 06905

May 4, 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 APISource, Inc. ("APISource") located at 7850 Walker Drive, Suite 400, Greenbelt, MD 20770, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. 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, APISource 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 March 24, 2020, APISource was alerted to suspicious activity on a website that it processes online orders through for its customers. APISource immediately began an investigation, with the assistance of a third-party forensic investigator, to assess the nature and scope of the incident. Through the investigation, it was determined that malicious code was present on the website from December 9, 2019 to March 26, 2020, and April 2, 2020 to April 3, 2020, which had the ability to capture customer information entered into the website while making a purchase. The information that could have been subject to unauthorized access includes name, address, payment card information and email address/password, if the consumer established an online account.

Notice to New Hampshire Resident

On or about May 4, 2020, APISource provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. 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, APISource moved quickly to investigate and respond to the incident, assess the security of APISource systems, and notify potentially affected individuals. APISource is also working to implement additional safeguards and training to its employees. APISource is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for one year through Kroll, at no cost to the individuals.

Additionally, APISource 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. APISource 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. APISource is also notifying any regulators of the incident as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

Gregory Bautista of
MULLEN COUGHLIN LLC

GJB:plm
Enclosure

EXHIBIT A

YOUR**LOOK**
YOUR**BRAND**
YOUR**SOURCE**

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

APISOURCE Inc. ("APISOURCE") is writing to inform you of an incident that may affect the security of some of your personal information, including your name and payment card information. APISOURCE is a branded merchandise company which provides ecommerce stores for various non-profit clients to sell merchandise to their members and supporters. While APISOURCE is not aware of any actual or attempted misuse of information, as a precaution, we are providing you with information about the incident, our response and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened? On March 24, 2020, APISOURCE was alerted to suspicious activity on a website that it processes online orders through for its customers. APISOURCE immediately began an investigation, with the assistance of a third-party forensic investigator, to assess the nature and scope of the incident. Through the investigation, it was determined that malicious code was present on the website from December 9, 2019 to March 26, 2020, and April 2, 2020 to April 3, 2020, which had the ability to capture customer information entered into the website while making a purchase. You are receiving a notice because you made a purchase on the website during this time frame.

What Information Was Involved? APISOURCE determined that the type of information potentially impacted by this incident includes your name, address, payment card information and email address/password, if you established an account.

What We Are Doing. APISOURCE takes the security of personal information in its care very seriously. APISOURCE reviewed its internal procedures and implemented additional safeguards on its website to protect customer information.

As an added precaution, APISOURCE is offering you access to one year of complimentary identity monitoring services through Kroll. The cost of this service will be paid for by APISOURCE. Instructions on how to activate the identity monitoring services can be found in the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud*.

What Can You Do? You can review the enclosed *Steps You Can Take to Help Protect Against Identity Theft and Fraud* for additional information on how to better help protect against identity theft and fraud. You can also activate the complimentary identity monitoring services described above.

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 1-844-978-2468, Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding major US holidays.

We sincerely apologize for this incident and regret any concern or inconvenience this has caused you.

Sincerely,

API Client Relations

Steps You Can Take to Help Protect Against Identity Theft and Fraud

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 30, 2020** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional considerations: The confidentiality, privacy and security of your personal information is one of our highest priorities. That's why we are sharing these steps you can take to protect your identity and uncover any fraudulent activity on 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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 one-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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

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, D.C. 20580, 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 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.

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

For Rhode Island residents, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 5 Rhode Island residents may be impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.