MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Julie Siebert-Johnson
Office: (267) 930-4005
Fax: (267) 930-4771
Email: jsjohnson@mullen.law

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

July 15, 2021

VIA FIRST-CLASS 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 ASIS International located at 1625 Prince Street, Alexandria, Virginia 22314, 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. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ASIS International 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

In May 2021, ASIS International identified suspicious activity on its e-commerce website. ASIS International promptly took steps to secure this system, including by removing the malicious code, and conducted an investigation aided by third-party forensic specialists. As a result of the investigation, it was discovered that malicious code was present between April 28, 2021 and May 6, 2021 that may have enabled an unauthorized party to obtain certain payment card information related to a limited number of transactions from the ASIS International e-commerce platform. Specifically, the investigated determined the vulnerability was contained in third-party code that was removed to prevent further exploitation. A comprehensive review of the information was conducted to determine any risk to payment card information from purchases during the specific timeframe. On June 23, 2021, ASIS International completed the investigation and identified and confirmed the population of individuals whose credit and/or debit card number and corresponding information may have been affected. ASIS International thereafter worked to provide this notification to potentially impacted individuals as quickly as possible.

The investigation determined that the malicious code was capable of collecting certain payment card information consisting of the cardholder's name and credit or debit card information including card number, expiration date, and cvv for payment cards used on the ASIS e-commerce platform during the specified dates above. This event only affected payment card information entered online during this timeframe as ASIS does not store credit card information.

Notice to New Hampshire Resident

On or about July 15, 2021, ASIS International began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, ASIS International moved quickly to investigate and respond to the incident, to assess the security of its systems, and to notify potentially affected individuals. ASIS International's response included working with the vendor to remediate the vulnerability exploited. ASIS International continues to assess additional measures to safeguard the information in its care, including increased system monitoring, alerting, and other system security measures. ASIS International also notified law enforcement of the event and has been cooperating with their investigation. Further, ASIS is notifying other regulatory authorities, as required.

Additionally, ASIS International is providing impacted individuals with guidance on how to 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. ASIS International is providing individuals with 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) 930-4005.

Very truly yours,

Julie Siebert-Johnson of
MULLEN COUGHLIN LLC

JSJ/ken

EXHIBIT A

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 15, 2021

G6096-L01-0000001 T00001 P001 ********SCH 5-DIGIT 32808
SAMPLE A. SAMPLE - L01 INDIVIDUAL
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Re: Notice Of Data [Variable1]

Dear Sample A. Sample:

ASIS International ("ASIS") is writing to notify you of an incident that may affect the security of certain payment card information. Please know that we value our customers and the privacy of the information in our care. We take this incident seriously and have been working diligently to investigate and respond. This letter provides you with information about the incident, our response, and steps you can take to protect against the possibility of identity theft and fraud, should you feel it is appropriate.

What Happened? In May 2021, we identified suspicious activity on our e-commerce website. We promptly took steps to secure this system including by removing the malicious code and conducted an investigation aided by third-party forensic specialists. As a result of the investigation, it was discovered that malicious code was present between April 28, 2021, and May 6, 2021 that may have enabled an unauthorized party to obtain certain payment card information related to a limited number of transactions from our e-commerce platform. Specifically, we determined the vulnerability was contained in third-party code and was removed to prevent further exploitation. A comprehensive review of the information was conducted to determine any risk to payment card information from purchases during the specific timeframe. On June 23, 2021, we completed the investigation and identified and confirmed the population of individuals whose information may have been affected. We thereafter worked to provide this notification to potentially impacted individuals as quickly as possible. We are notifying you because our records reflect that you made a transaction through our e-commerce platform during the above time period.

What Information Was Involved? Our investigation determined that the malicious code was capable of collecting certain payment card information consisting of the cardholder's name and credit or debit card information including card number, expiration date, and cvv for payment cards used on the ASIS e-commerce platform during the specified dates above. This event only affected payment card information entered online during this timeframe as we do not store credit card information.

What We Are Doing. Our priority is preserving the privacy and trust of our members and customers, whether in-person or using our e-commerce platform, and we moved swiftly to address this issue. Our response included working with the vendor to remediate the vulnerability exploited. We review our security measures against the highest Payment Card Industry compliance requirements. Additionally, while we have security measures in place to protect your data, we continue to assess additional measures to safeguard the information in our care, including increased system monitoring, alerting, and other system security measures. We also notified law enforcement of the event and have been cooperating with their investigation. Further, we are notifying regulatory authorities, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity to detect errors. You may also request that your bank issue you a new payment card as a precaution. We also encourage you to report any suspicious activity to law enforcement. Additional information may also be found in the enclosed "Steps You Can Take To Help Protect Personal Information" section of this letter.

For More Information. We understand that you may have questions that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated call center at (855) 252-2731, which is available from 9:00 AM to 11:00 PM Eastern Time Monday through Friday, or 11:00 AM to 8:00 PM Eastern Time Saturday and Sunday (excluding major U.S. holidays). Please be prepared to provide Engagement Number B015890 when speaking with an agent. Additionally, you may contact ASIS at data-event@asisonline.org.

We sincerely regret any inconvenience or concern this event may cause you. We remain committed to safeguarding customer information, and will continue to take steps that ensure the security of our systems including our e-commerce site.

Sincerely,

Peter O'Neil
Chief Executive Officer
ASIS International

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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 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, D.C. 20001; 202-727-3400; and 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 www.oag.state.md.us. ASIS International is located at 1625 Prince Street, Alexandria, Virginia 22314.

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 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 https://ag.ny.gov/.

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 www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 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 is approximately 1 Rhode Island resident impacted by this incident.