



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

APR 06 2020

CONSUMER PROTECTION

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 31, 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 the National Institute for Automotive Service Excellence (“ASE”) located at 1503 Edwards Ferry Road, NE, Suite 401, Leesburg, Virginia 20176 and are writing to notify your office of an incident that may affect the security of certain customer payment card information. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ASE 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

ASE began investigating recent reports from a small number of customers who made purchases from <https://portal.asecrm.com>. In response, ASE worked with an outside forensics expert to investigate these reports to determine what may have happened. Through this investigation, ASE confirmed on February 13, 2020, that an unauthorized actor placed malicious code on ASE’s checkout page, which could capture customer payment card information when entered on the checkout page for transactions between December 18, 2019, to February 3, 2020, and February 4, 2020, to February 13, 2020. ASE immediately worked to remove the malicious code to prevent any further issues. Customers can safely and securely use their payment card at ASE’s website.

The investigation determined the code potentially captured cardholder information including name, address, cardholder name, credit card number, expiration date, and CVV code between December 18, 2019 and February 3, 2020, and February 4, 2020, and February 13, 2020.

Notice to New Hampshire Residents

On or about March 31, 2020, ASE began providing written notice of this incident to individuals who provided payment card information on <https://portal.asecrm.com> between December 18, 2019 and February 3, 2020, and February 4, 2020 and February 13, 2020, which includes seventy seven (77) 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

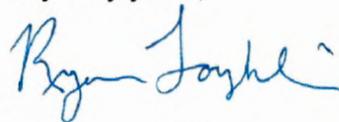
Upon discovering the event, ASE moved quickly to investigate and respond to the incident, assess the security of ASE systems, and notify potentially affected individuals. ASE is also working to review existing policies and procedures.

Additionally, ASE 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. ASE 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) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL: amw
Enclosure

EXHIBIT A



National Institute for
AUTOMOTIVE SERVICE EXCELLENCE

Date

[First Name] [Last Name]

[Address 1]

[City, State Zip]

Re: Notice of Data Breach

Dear [First Name][Last Name]:

The National Institute for Automotive Service Excellence (“ASE”) is writing to notify you of an incident that may have impacted your payment card information. We are providing you with information about the event, our response, and steps you may take to better protect against the possible misuse of your information, should you feel it appropriate to do so.

What Happened? ASE began investigating recent reports from a small number of customers who made purchases from <https://portal.asecrm.com>. In response, ASE worked with an outside forensics expert to investigate these reports to determine what may have happened. Through this investigation, ASE confirmed on February 13, 2020, that an unauthorized actor placed malicious code on ASE’s checkout page, which could capture customer payment card information when entered on the checkout page for transactions between December 18, 2019, to February 3, 2020, and February 4, 2020, to February 13, 2020. ASE immediately worked to remove the malicious code to prevent any further issues. You can safely and securely use your payment card at our website.

What Information was Involved? Your information was provided to ASE because of purchases you made from ASE’s website. The investigation determined the code potentially captured information including your name, address, card holder name, credit card number, expiration date, and CVV code for certain transactions from December 18, 2019, to February 3, 2020, and February 4, 2020, to February 13, 2020.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among ASE’s highest priorities. Upon learning of the event, we investigated to determine what happened, identified those individuals who may be affected, secured the webpage, and will be taking additional steps to further secure the website.

What You Can Do. If you see any unauthorized activity on your credit card or debit card statements, promptly contact your bank, credit union, or credit card company. Please review the enclosed *Steps You Can Take to Protect Your Information*, which contains information on what you can do to better protect against possible misuse of your information.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions or concerns regarding this incident, please call [NUMBER], [CALL CENTER HOURS] (excluding U.S. holidays).

Sincerely,



Timothy A. Zilke

President & CEO

National Institute for Automotive Service Excellence



Steps You Can Take to Protect Against Identity Theft and Fraud

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 PO Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	Equifax PO Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	--	---

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 2002 Allen, TX 75013 1-888-397-3742 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	Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 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, DC 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 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.

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 Rhode Island Residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; 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 62 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 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 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/>.