



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Christopher J. DiLenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdilenno@mullen.law

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

January 5, 2022

VIA E-MAIL

Office of the Attorney General
Security Breach Notification
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

Dear Sir or Madam:

We represent Smith System Driver Improvement Institute, Inc. (“Smith System”) located at 2301 East Lamar Blvd., Suite 250 Arlington, TX 76006, and are writing to notify your office of an incident that may affect the security of some personal information relating to thirteen (13) Maryland residents. 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, Smith System does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about September 30, 2021, Smith System discovered suspicious activity on its website. In response, Smith System worked with outside specialists to investigate the nature and scope of the activity, and secure its systems. Smith System determined an unauthorized actor had installed malicious code on its website, DriveDifferent.com, to record and exfiltrate credit card information entered onto the Smith System online webstore likely beginning November 25, 2020, and ending on November 17, 2021. Smith System removed the malicious code from its website and has taken steps to ensure its systems are secure. Smith System reviewed the transactions processed on its webstore during the timeframe in question. On November 24, 2021, Smith System determined that personal information relating to Maryland residents may have been impacted. The types of personal information impacted were names, credit card numbers, expiration dates, CVV codes, and billing addresses relating to credit cards used on the DriveDifferent.com website between

November 25, 2020, and November 17, 2021, potentially relating to thirteen (13) Maryland residents.

Notice to Maryland Residents

On or about January 5, 2022, Smith System provided written notice of this incident to affected individuals, which includes thirteen (13) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. We do note that all of the involved credit cards appear to belong to various companies and are therefore corporate cards, not personal, individual cards, but this cannot be confirmed so we are notifying the card holders.

Other Steps Taken and To Be Taken

Upon discovering the event, Smith System moved quickly to investigate and respond to the incident, assess the security of Smith System systems, and notify potentially affected individuals. Smith System is also working to implement additional safeguards and training to its employees.

Additionally, Smith System 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. Smith System 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) 930-4775.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/rzh
Enclosure

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 Security Event

Dear <<Name 1>>:

The Smith System Driver Improvement Institute, Inc. ("Smith System") is writing to notify you of a recent incident that may have impacted the security of credit card information used on our website, DriveDifferent.com. We want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

What Happened? On or around September 30, 2021, Smith System discovered the presence of suspicious activity on its website. In response, Smith System worked with an outside forensics specialist to investigate the nature and scope of the activity. The investigation determined that an unauthorized actor had accessed the Smith System website and installed malicious code to record credit card information being entered onto the Smith System online store, sometime between November 25, 2020, and November 17, 2021. Smith System promptly removed all the malicious code and secured its systems. Every potentially impacted transaction was then reviewed to determine the scope of this incident. On November 24, 2021 we determined that you conducted a transaction on behalf of <<Variable data 2/Company>>, on our online store, DriveDifferent.com, during this timeframe.

What Information was Involved? The investigation determined that the name, credit card number, CVV code, billing address and expiration date relating to a credit card used on the DriveDifferent.com website between November 25, 2020, and November 17, 2021, might have been accessed by the unauthorized actor. While this information might have been accessed, at this time we have no indication that this information was actually used.

What We Are Doing. The confidentiality, privacy, and security of personal information within our care is among Smith System's highest priorities. Upon learning of the event, we investigated to determine those individuals that were affected, and secured our systems by deleting all malicious code on our website. The Smith System servers have been thoroughly scanned and reviewed for any additional vulnerability. We will be taking additional steps to improve security and better protect against similar incidents in the future.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Personal 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, please call 855-604-1722, Monday through Friday 8:00 AM to 8:00 PM (Central).

Sincerely,

Tony Douglas
CEO

STEPS YOU CAN TAKE TO 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, D.C. 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.

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 violators. 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. NW, 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.