



MULLEN
COUGHLIN_{LLC}

STATE OF NH
DEPT OF JUSTICE
2017 JAN 17 AM 11:35

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

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 9, 2017

Via U.S. Mail

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attention: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Event

Dear Attorney General Foster:

We represent LightYear Dealer Technologies: DealerBuilt ("DealerBuilt"), 2570 4th Street SW, Suite A, Mason City, Iowa 50401. We are writing to notify you of a data security incident that may have compromised the security of personal information of New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, DealerBuilt does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Security Event

DealerBuilt provides dealer management services to certain automobile dealerships throughout the country. As part of these services, DealerBuilt hosts backups of dealership data in a secondary repository for recovery purposes in case of an on-site catastrophe. On Monday, November 7, 2016, DealerBuilt learned of a vulnerability within the process being utilized to back up dealership data, which resulted in backup data related to certain dealerships being accessible via the internet.

Upon learning of this incident, DealerBuilt immediately began taking steps to investigate and mitigate this vulnerability including changing the backup process to prevent unsecured access from the internet and shutting off the affected server while these changes are being made. DealerBuilt also retained third party computer forensic investigators to assist with determining what, if any, information may have been exposed through this vulnerability. This investigation has determined

that a limited amount of backup data related to certain dealerships was acquired without authorization between October 29, 2016 and November 7, 2016. While it appears that the data may have been acquired during a security researcher's review of the backup process, our investigation is unable to specifically identify who may have acquired the data.

DealerBuilt provided notice of this incident to impacted dealers beginning on November 18, 2016. Since that time, DealerBuilt has been working with the third party computer forensic instigators to identify those individuals impacted by this incident. While DealerBuilt's investigation into this event is ongoing, it has determined that the impacted backup data may have contained the following information for impacted individuals: name, date of birth, Social Security number, driver's license number, credit card number, and/or financial account number. The backup data may have also contained corporate financial account numbers if that information was stored in the dealership data that was being backed up by DealerBuilt.

Notice to New Hampshire Residents

On January 9, 2016, DealerBuilt will begin mailing notice letters to potentially affected individuals which includes twenty-six (26) New Hampshire residents. The notice will be provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

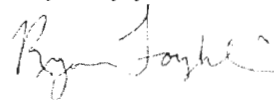
In addition to providing written notice of this incident to all affected individuals on behalf of the affected dealerships as described above, DealerBuilt is offering all affected New Hampshire residents one year of credit monitoring and identity restoration services with Experian ProtectMyID. DealerBuilt is also providing written notice of this incident to other state regulators and consumer reporting agencies, where required.

DealerBuilt is taking steps to mitigate the risk that an event like this happens again. In addition to utilizing third-party forensic experts to investigate this incident, DealerBuilt also retained a separate IT firm to assist with a security audit of its systems. As part of its ongoing commitment to the security of the information in its care, DealerBuilt has implemented additional measures to further protect its systems.

Contact Information

Should you have any questions regarding this notification or other aspects of this event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

EXHIBIT A



Return Mail Processing
P.O. Box 442
Claysburg, PA 16625-0442



123456

##C4812-L01-0123456

SAMPLE A SAMPLE

123456

APT ABC

123 ANY ST

ANYTOWN US 12345-6789



January 9, 2017

RE: Notice of Data Breach

Dear Sample A Sample:

We are writing to notify you of a recent incident involving certain personal information related to you. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? As part of our services, LightYear Dealer Technologies, LLC (“DealerBuilt”) hosts backups of car dealership data in a secondary repository for recovery purposes in case of an on-site catastrophe. On Monday, November 7, 2016, DealerBuilt learned of a vulnerability with the process being utilized to back up dealership data. This vulnerability made dealership backup data accessible if certain steps were taken. DealerBuilt immediately began taking steps to investigate and mitigate the impact of this vulnerability, including changing the backup process to eliminate this vulnerability and shutting off the affected server while these changes are made. We also retained third party computer forensic investigators to assist with determining what, if any, information may have been exposed through this vulnerability. Our investigation has determined that a limited amount of back up data was acquired without authorization between October 29, 2016 and November 7, 2016. While it appears that the data may have been acquired during a security researcher’s review of the backup process, our investigation is unable to specifically identify who may have acquired the data.

What Information Was Involved? DealerBuilt determined that the impacted backup data contained the following information related to you: name and credit card number.

What We Are Doing. DealerBuilt takes the security of the personal information in our care very seriously. In addition to launching an investigation into this incident with third party computer forensic investigators, we also retained a separate IT security firm to assist with a security audit of our systems. As part of our ongoing commitment to the security of the information in our care, we have implemented additional measures to further protect our systems and the information provided to us. We are also providing you with information you can use to better protect against identity theft and fraud, as well as access to one year of credit monitoring and identity restoration services at no cost to you.

What You Can Do. You can review the enclosed *Steps You Can Take to Prevent Identity Theft and Fraud* for more information on ways to protect against the potential misuse of your personal information. You can also enroll to receive the complimentary credit monitoring and identity restoration services.

For More Information. Again, we take the security of personal information in our care very seriously. We apologize for any inconvenience or concern this incident may cause you. We understand that you may have questions that are not addressed in this letter. If you have any questions or concerns please do not hesitate to contact our dedicated assistance line at (877) 237-9502 between 9:00 AM – 7:00 PM EST Monday through Friday, excluding major holidays. Please provide reference number **5958122716** when calling.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike Trasatti". The signature is fluid and cursive, with a large initial "M" and "T".

Mike Trasatti
CEO
LightYear Dealer Technologies, LLC dba DealerBuilt

Enclosure



123456

Steps You Can Take to Prevent Identity Theft and Fraud

To help you further safeguard against any potential misuse of your personal information, we are offering you access to one year of complimentary credit monitoring and identity restoration services with Experian ProtectMyID.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that fraud resolution support is needed then an Experian Fraud Resolution agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition.)

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID[®] Alert as a complimentary one year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

Ensure that you **enroll by: January 6, 2018** (Your code will not work after this date.)

Visit the ProtectMyID website to enroll: www.protectmyid.com/alert

Provide your **activation code: XXXXXXXXXXX**

If you have questions about the incident, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-297-7780 by January 6, 2018. Be prepared to provide engagement number **PC105721** as proof of eligibility for the fraud resolution services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ONE YEAR PROTECTMYID MEMBERSHIP:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian file for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE:** You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.

- **\$1 Million Identity Theft Insurance¹:** Provides coverage for certain costs and unauthorized electronic fund transfers.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms 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.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze

In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for the previous two years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. Fees vary based on where you live, but commonly range from \$5 to \$10.

¹ Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



123456

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting 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. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General. 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 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 of identity theft. **Maryland** residents may contact the MD Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202. **North Carolina** residents may contact the NC Attorney General's Office, Consumer Protection Division, at 1-877-566-7226, www.ncdoj.com, or 9001 Mail Service Center, Raleigh, NC 27699. **Rhode Island** residents may contact the RI Attorney General's Office at (401) 274-4400, <http://www.riag.ri.gov/>, or 150 South Main Street, Providence, RI 02903. There are three (3) Rhode Island residents affected by this incident. This notice was not delayed as a result of a law enforcement investigation.