

Cynthia J. Larose
617 348 1732
cjlarose@mintz.com



One Financial Center
Boston, MA 02111
617 542 6000
mintz.com

February 9, 2022

VIA E-MAIL TRANSMISSION (IDTHEFT@OAG.STATE.MD.US)

Attorney General Brian E. Frosh
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Reporting of Security Incident Pursuant to Maryland Code. § 14-3505

Dear Attorney General Frosh:

We are writing on behalf of The Lyon Waugh Auto Group (the "Company") to advise you of an incident that may affect the security of personal information relating to approximately 5 Maryland residents. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

The Company was alerted on December 4, 2021 that a malicious actor had exploited a vulnerability and disabled the Company's security products to gain access to certain Company systems as well as various network resources and files in an apparent ransomware attack. Upon learning of the incident, the Company immediately took steps to isolate and secure its systems and investigate the incident. Also on December 4, the Company retained a nationally-known third-party forensics firm to determine the nature and scope of the intrusion. The Company also reported indicators of compromise detected in the incident to the FBI.

In the course of the investigation and restoration work, the Company was able to restore its files from backup and no ransom was paid. Through the Company's continued investigation, on January 7, 2022, the Company became aware that the attacker accessed and potentially exfiltrated files containing personal information, and since then, has been working diligently to identify which files and which individuals may have been affected. As a result of the Company's internal investigation, it was determined that the files accessed and potentially exfiltrated by the attacker contained personal information including name, address, email address, and Social Security number of certain current and former Company employees, including 5 Maryland residents.

The Company is taking this incident very seriously, and has taken a number of steps to strengthen the protection of personal information and mitigate risk to protect from further types of attacks, including resetting all user credentials and extending its implementation of multi-factor authentication. In addition, the Company rebuilt certain systems and retired others. The Company continues to closely monitor its network and information systems for unusual activity. The Company will also continue to further improve security across the Company networks and protect from unauthorized access or similar criminal activity in the future.

The Company is not aware of any fraudulent use of personal information of the affected Maryland residents at this time. The Company is sending the attached notice to affected Maryland residents on February 9, 2022, and the Company has arranged to make credit monitoring and identity protection services by IDX available to them at no cost for two (2) years. This includes access to assist individuals

MINTZ

Office of Attorney General
February 9, 2022
Page 2



with credit restoration, a \$1,000,000 insurance reimbursement policy, and credit monitoring services as described in the attached form of notice.

Please contact the undersigned at cjlarose@mintz.com or 617-348-1732 should you need further information or have any additional questions.

Sincerely,

A handwritten signature in black ink, appearing to read 'Cynthia J. Larose'. The signature is fluid and cursive, with the first name 'Cynthia' and last name 'Larose' being clearly distinguishable.

Cynthia J. Larose
Member

Attachments

The Lyon Waugh Auto Group
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:
1-833-676-2144
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<To the Family of>><<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

February 9, 2022

Notice of Data Incident

Dear <<Family of>><<First Name>> <<Last Name>>,

What Happened

We are writing to inform you of an incident that may have affected your personal information.

As you may be aware, on December 4, 2021, we first learned of a cyberattack that partially disrupted Lyon Waugh's information systems. Upon learning of the incident, we immediately took steps to isolate and secure our systems and investigate the incident. We retained a third-party forensics firm and a third-party IT managed services firm to secure our systems, remediate any risks, and methodically bring our systems back online. As part of the investigation, on January 7, 2022, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems, including documents that may have contained some of your personal information. Since then, we have been analyzing impacted files to understand what personal information may be at risk, and working to provide notice to individuals and authorities, as applicable.

What Information Was Involved

The type of information differs from individual to individual, but may have included your name, address, date of birth, Social Security number, insurance and other benefits information. You may be receiving this letter as the spouse or dependent of an employee or former employee of The Lyon Waugh Auto Group.

What We Are Doing

Upon learning of the incident, we engaged a well-known forensic investigation firm to identify the scope of the incident and to assist us with securing our systems and data. We have carefully brought our systems back online and we continue to closely monitor our network and information systems for unusual activity. We have also engaged a third-party managed IT services firm to assist us with the restoration of our systems and additional resources. We will continue to further improve security across our company networks and protect from unauthorized access or similar criminal activity in the future.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. To receive credit services, you must be over the age of 18, 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. If you do not have a credit file, you will not be able to register for credit monitoring services, but you will receive CyberScan monitoring, insurance, and the fully managed identity recovery services from IDX.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-676-2144 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is May 9, 2022.

At this time, we have not received any reports that personal information has been subject to fraudulent activity. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Additional Important Information document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-833-676-2144 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Warren Waugh, Jr.

Warren Waugh, Jr.
Managing Partner
The Lyon Waugh Auto Group

(Enclosure)



Additional Important Information

- 1. Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-833-676-2144 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity 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. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

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

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may 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 5 years, provide the addresses where you have lived over the prior 5 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, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were <<X>> Rhode Island residents impacted.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.