Freeman Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

July 18, 2024

Via Email Only
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: IDtheft@oag.state.md.us

Re: Jim Ellis Auto Group – Notice of Data Event

Dear Sir or Madam:

We represent Jim Ellis Auto Group, a family of car dealerships serving the Atlanta, Georgia metropolitan area and surrounding communities. This letter is provided pursuant to the Maryland Personal Information Protection Act, MD. CODE ANN. COM. LAW § 14-3501, *et seq*, which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of Maryland.

On or about January 25, 2024, the JEAG dealership group computer networks were disrupted by computer malware, forcing it to take its systems offline. JEAG partnered with data incident response specialists to restore its systems safely and conduct an investigation into the nature and scope of the event. On or about February 7, 2024, JEAG learned that certain data was taken from its network during the event. JEAG therefore commenced a thorough review of that data which concluded on June 12, 2024. While JEAG has no knowledge of any actual or attempted misuse of information at this time, it is notifying those potentially impacted by this event. The data points that could have been impacted include Social Security number, driver's license number, and financial account information.

On July 17, 2024, JEAG provided notice to the potentially affected individuals by U.S. regular mail. JEAG provided this notification to 2,275 individuals, including four (4) residents of the State of Maryland. A sample copy of the notice letter is attached here as ***Exhibit A***.

JEAG is providing written notice of the event that includes a brief description of the incident, encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, immediately reporting errors or suspicious activity to the financial institution or service provider, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered, from any source. JEAG enclosed documentation containing contact information for the major consumer reporting bureaus, state-specific regulators, an incident-specific call center, and additional steps individuals may take to protect their information from misuse, should they find it appropriate to do so. JEAG is offering twelve (12) months of identity theft monitoring and restoration services through IDX. The monitoring services include single bureau credit and CyberScan monitoring, fully managed ID theft recovery services, and access to a $1 million dollar insurance reimbursement policy.

JEAG takes this event and the security of personal information entrusted to it very seriously and has taken steps to help mitigate the potential for harm and prevent this from happening again. JEAG partnered with data incident response specialists to thoroughly investigate the event and provide notice to those potentially impacted. JEAG reported the event to federal law enforcement. JEAG continues to utilize complex password requirements and will continue to review its existing security measures in place for ways to defend against future threats. JEAG is also notifying other regulators as required.

I believe this provides you with all information necessary for your purposes and to comply with Maryland law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

/s/ Nicholas Jajko

Nicholas Jajko

Freeman Mathis & Gary LLP

Exhibit A

P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:

https://app.idx.us/account-creation/protect

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

July 17, 2024

Re: Notice of Data <<Variable Data 2>>

Dear <<First Name>> <<Last Name>>:

We at Jim Ellis Auto Group take the privacy and security of personal information seriously. As part of that commitment, we are notifying you of an event that impacted our computer network. Please read this letter carefully.

What Happened?

On or about January 25, 2024, our dealership group computer networks were disrupted by computer malware, forcing us to take our systems offline. We partnered with data incident response specialists to restore our systems safely and conduct an investigation into the nature and scope of the event. On or about February 7, 2024, we learned that certain data was taken from our network during the event. We therefore commenced a thorough review of that data which concluded on June 12, 2024. While we have no knowledge of any actual or attempted misuse of your information at this time, we believe it is important to notify those potentially impacted by this event.

What Information Was Involved?

Our review of the potentially impacted data confirmed that your <<Variable Data 1>> were present on our network servers and could have been taken during the event. We reiterate that we have no knowledge of any actual or attempted misuse of your information at this time.

What We Are Doing.

We take this event and the security of personal information entrusted to us very seriously and have taken steps to help mitigate the potential for harm and prevent this from happening again. We partnered with data incident response specialists to thoroughly investigate the event and provide notice to those potentially impacted. We reported the event to federal law enforcement. We continue to utilize complex password requirements and will continue to review our existing security measures in place for ways to defend against future threats.

As an additional resource, we are offering you a complimentary <<twelve (12)/twenty-four (24)>> month membership of credit monitoring and identity theft protection services through IDX, A ZeroFox Company. This includes single bureau credit and CyberScan monitoring, fully managed ID theft recovery services, and access to a one-million-dollar ($1,000,000) insurance reimbursement policy. With this protection, IDX will help you resolve issues if you suspect your identity is compromised. Instructions for how to enroll are below. Additional information about these services is also enclosed.

What You Can Do.
We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or the appropriate service provider. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation titled "Additional Steps to Help Protect Your Information" for contact information and resources you may take advantage of to protect against fraud or misuse, should you find it appropriate to do so.

You may enroll and take advantage of the offered IDX identity protection services by going to https://app.idx.us/account-creation/protect or calling 1-800-939-4170 or scanning the QR code and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am – 9 pm Eastern Time. Please note the deadline to enroll is October 17, 2024.

For More Information.
Jim Ellis Auto Group is very sorry for any concern or inconvenience this event has caused or may cause you, but please know that we remain committed to protecting the information entrusted in our care. If you have any other questions or concerns you may contact our dedicated call center at 1-800-939-4170, Monday through Friday from 9 am – 9 pm Eastern Time, excluding major holidays.

Sincerely,

Stacey Ellis Hodges

Stacey Ellis Hodges
Jim Ellis Auto Group

ADDITIONAL STEPS TO HELP PROTECT YOUR INFORMATION

Review Personal Account Statements and Credit Reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. 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 (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, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report Suspected Fraud. 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 should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts will last one year. Fraud alerts are free and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide credit reporting agencies by phone or online using the above contact information. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online using the above contact information. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain Additional Information about the steps you can take to avoid identity theft from the following entities:

- **District of Columbia Residents:** District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington D.C. 20001; https://oag.dc.gov; and (202) 727-3400;
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.marylandattorneygeneral.gov, and toll-free at (888) 743-0023 or (410) 528-8662;
- **New York Residents:** New York Attorney General may be contacted at Office of Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, and (800) 771-7755;
- **North Carolina Residents:** Office of the Attorney General of North Carolina may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.gov, (919) 716-6400;
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338). This notification was not delayed by law enforcement.

1. Website and Enrollment. Scan the QR image or 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 1-800-939-4170 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. 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.

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.

IDX Identity enrollments will include <<12/24>> months of the following service components:

SINGLE BUREAU CREDIT MONITORING (adults) - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.