

May 27, 2020

Via Email and FedEx

Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notification of Personal Information Security Breach

Dear Sir/Madam:

This notification is submitted on behalf of Icahn Automotive Group LLC (“IAG”). IAG owns and operates auto supply, repair and maintenance stores, including Pep Boys® automotive aftermarket retail and service chain, Auto Plus® automotive aftermarket parts distributor, Precision Tune Auto Care® owned automotive service centers, and AAMCO Total Auto Care owned service centers. IAG’s address is 112 Townpark Drive NW, Suite 300, Kennesaw, Georgia 30144.

I write regarding a data incident involving the personal information maintained by IAG about its employees and certain other individuals. On or about April 6, 2020, IAG discovered that an unauthorized actor had gained access to an employee’s email account. Promptly after discovering the unauthorized access, the employee’s email account was locked down and the password was changed. IAG’s investigation revealed that the actor obtained access to the email account on or about approximately March 13, 2020, and that the access ceased on or before April 4, 2020.

IAG and its outside counsel engaged a forensics firm to determine whether and to what extent information in the account may have been accessed or acquired. As of the date of this letter, IAG has no evidence that the actor used or disseminated any personal information acquired or that obtaining such information was the reason for the intrusion. Furthermore, IAG’s forensic consultant firm confirmed that the information exposed to the actor could not be located on any of the typical websites known to store or sell misappropriated personal information. Furthermore, to prevent similar occurrences from happening in the future, IAG is taking security measures to further bolster the security of the information it holds.

Based upon the information available to it, IAG believes the personal information of approximately eight New Hampshire residents was potentially exposed in the incident. On May 14, 2020, after additional investigation, IAG learned that the personal information of approximately 229 additional New Hampshire residents was potentially exposed in the incident, and it notified such individuals on May 21, 2020. On May 22, 2020, IAG learned that the personal

Craig.Foster@ThompsonHine.com Phone 614.469.3280 Fax 614.469.3361

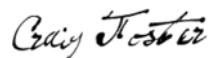
information of approximately two additional New Hampshire residents was potentially exposed in the incident, and it notified such individuals on that date.

While the type of information stored on the compromised email account varied from person to person, the information generally included some combination of name, employee ID number, driver's license number, financial account number, date of birth, address, work location, compensation and benefit information, dates of employment, social security number, and claims information.

Samples of the notices sent to the affected New Hampshire residents on May 6, 2020, May 21, 2020 and May 22, 2020 are enclosed with this notice. As described in the samples, New Hampshire residents are being offered credit monitoring, fraud consultation and identity theft restoration services for 12 months. Notification is not being delayed as a result of a law enforcement investigation.

IAG takes this matter seriously and is continuing to work to protect the personal information it holds. Please let me know if you would like to discuss the incident further.

Sincerely,



Craig Foster



Icahn Automotive Group LLC
112 Townpark Dr NW – Ste 300
Kennesaw, GA 30144

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you regarding an incident involving certain information we maintain about you. While we have no evidence that your information was actually used, we take this event very seriously and we feel it is important to inform you of what happened, what we have done in response and what you can do to help protect yourself. Please read this letter carefully and contact us with any questions as instructed below.

What Happened

On or about April 6, 2020, we discovered that an unauthorized actor had gained access to an employee's email account. Promptly after discovering the unauthorized access, access to the employee's email account was blocked. Our investigation revealed that the actor obtained access to the email account on or about approximately March 13, 2020, and that the access ceased on or before April 4, 2020. We have engaged a forensics firm to determine whether and to what extent information in the account may have accessed or acquired.

Our investigation has determined the compromised email account contained personal information relating to you. We have no evidence that the intruder used or disseminated your information or that obtaining such information was the reason for the intrusion. Furthermore, as of today, our forensic consultant firm confirmed that the information exposed to the intruder could not be located on any of the typical websites known to store or sell misappropriated personal information.

What Information Was Involved

While the type of information stored on the compromised email account varied from person to person, the information generally included some combination of name, employee ID number, driver's license number, financial account number, date of birth, address, work location, compensation and benefit information, dates of employment, claims information, and Social Security number.

What We Are Doing

To prevent similar occurrences from happening in the future, we are taking security measures to further bolster the security of the information we hold. We have not delayed this notification as a result of a law enforcement investigation.

What You Can Do

We encourage you to take preventative measures now to help prevent and detect any misuse of your information such as placing a fraud alert and/or security freeze on your credit file, performing a review of your credit reports, and enrolling in free identity monitoring services.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit reporting agency confirms your fraud alert, the other major agencies are notified to place similar fraud alerts on your credit file. You may also decide to request a security freeze, which prevents a credit reporting agency from releasing your credit report without your consent. You may contact any one of the three major credit reporting agencies or the Federal Trade Commission to obtain additional information about fraud alerts and/or security freezes.



You are entitled to one free copy of your credit report every 12 months from each of the three major credit reporting agencies. We recommend you closely monitor your financial accounts and credit reports for incidents of fraud and identify theft, and, if you see any unauthorized activity, promptly contact your financial institution.

Equifax
(www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111

Experian
(www.experian.com)
P.O. Box 2390
Allen, TX 75013
1-888-397-3742

TransUnion
(www.transunion.com)
P.O. Box 1000
Chester, PA 19016
1-800-888-4213

In addition, we have arranged with Kroll to provide you with identity monitoring for 12 months, which we will provide at no cost to you. Your identity monitoring services include Single Bureau Credit Monitoring, Fraud Consultation and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **August 7, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you remain vigilant for incidents of fraud or identity theft by checking your credit reports and account statements periodically. Checking these documents periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should take action. Such action may include contacting the credit reporting agencies and your financial institution(s), contacting law enforcement, including your state's attorney general and the Federal Trade Commission, and filing a police report. You should get a copy of the report since many creditors want the information it contains to resolve fraudulent debts. You also may file a complaint with the FTC.

For More Information

Additionally, the FTC offers consumer assistance and educational materials relating to steps individuals can take to avoid identity theft and privacy issues. The FTC may be contacted at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 382-4357
www.ftc.gov/idtheft

If you have any questions about this notification or require further assistance, please feel free to contact us Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time **excluding major US holidays** at **1-866-377-0061**.

Sincerely,

Liviu Dedes
SVP HR, Chief People Officer

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and 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.



Icahn Automotive Group LLC
112 Townpark Dr NW – Ste 300
Kennesaw, GA 30144

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are contacting you regarding an incident involving certain information we maintain about you. While we have no evidence that your information was actually used, we take this event very seriously and we feel it is important to inform you of what happened, what we have done in response and what you can do to help protect yourself. Please read this letter carefully and contact us with any questions as instructed below.

What Happened

On or about April 6, 2020, we discovered that an unauthorized actor had gained access to an employee's email account. Promptly after discovering the unauthorized access, access to the employee's email account was blocked. Our investigation revealed that the actor obtained access to the email account on or about approximately March 13, 2020, and that the access ceased on or before April 4, 2020. We have engaged a forensics firm to determine whether and to what extent information in the account may have accessed or acquired.

Our investigation has determined the compromised email account contained personal information relating to you. We have no evidence that the intruder used or disseminated your information or that obtaining such information was the reason for the intrusion. Furthermore, as of today, our forensic consultant firm confirmed that the information exposed to the intruder could not be located on any of the typical websites known to store or sell misappropriated personal information.

What Information Was Involved

While the type of information stored on the compromised email account varied from person to person, the information generally included some combination of name, employee ID number, driver's license number, financial account number, date of birth, address, work location, compensation and benefit information, dates of employment, and Social Security number.

What We Are Doing

To prevent similar occurrences from happening in the future, we are taking security measures to further bolster the security of the information we hold. We have not delayed this notification as a result of a law enforcement investigation.

What You Can Do

We encourage you to take preventative measures now to help prevent and detect any misuse of your information such as placing a fraud alert and/or security freeze on your credit file, performing a review of your credit reports, and enrolling in free identity monitoring services.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit reporting agency confirms your fraud alert, the other major agencies are notified to place similar fraud alerts on your credit file. You may also decide to request a security freeze, which prevents a credit reporting agency from releasing your credit report without your consent. You may contact any one of the three major credit reporting agencies or the Federal Trade Commission to obtain additional information about fraud alerts and/or security freezes.



You are entitled to one free copy of your credit report every 12 months from each of the three major credit reporting agencies. We recommend you closely monitor your financial accounts and credit reports for incidents of fraud and identify theft, and, if you see any unauthorized activity, promptly contact your financial institution.

Equifax
(www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111

Experian
(www.experian.com)
P.O. Box 2390
Allen, TX 75013
1-888-397-3742

TransUnion
(www.transunion.com)
P.O. Box 1000
Chester, PA 19016
1-800-888-4213

In addition, we have arranged with Kroll to provide you with identity monitoring for 12 months, which we will provide at no cost to you. Your identity monitoring services include Single Bureau Credit Monitoring, Fraud Consultation and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

*You have until **August 7, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission recommends that you remain vigilant for incidents of fraud or identity theft by checking your credit reports and account statements periodically. Checking these documents periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should take action. Such action may include contacting the credit reporting agencies and your financial institution(s), contacting law enforcement, including your state's attorney general and the Federal Trade Commission, and filing a police report. You should get a copy of the report since many creditors want the information it contains to resolve fraudulent debts. You also may file a complaint with the FTC.

For More Information

Additionally, the FTC offers consumer assistance and educational materials relating to steps individuals can take to avoid identity theft and privacy issues. The FTC may be contacted at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) 382-4357
www.ftc.gov/idtheft

If you have any questions about this notification or require further assistance, please feel free to contact us Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time **excluding major US holidays** at **1-866-377-0061**.

Sincerely,

Liviu Dedes
SVP HR, Chief People Officer

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and 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.