



CORPORATE OFFICE

3200 MANCHESTER TRFWY.
KANSAS CITY, MO 64129

(800) 827-7694 / (816) 923-5000
FAX: (816) 923-9000

January 7, 2021

BY Email

Office of the Attorney General
Consumer Protection Bureau
33 Capitol St.
Concord, NH 03301
attorneygeneral@doj.nh.gov

To Whom It May Concern:

On behalf of Arrow Truck Sales, Inc. ("Arrow"), and pursuant to N.H. Rev. Stat. § 359-C:20, this letter provides notice of a cybersecurity incident. Arrow is a retailer of pre-owned medium- and heavy-duty trucks operating primarily in the United States and Canada. Arrow is a for-profit entity incorporated in Missouri and has its headquarters in Kansas City, MO.

On or about November 30, 2020, Arrow experienced a ransomware incident. We discovered the incident after Arrow personnel reported being unable to access Arrow's servers and that their login credentials had been changed. On December 17, 2020, Arrow determined that personal information may have been affected.

After becoming aware of the incident, we quickly began a thorough investigation with the support of outside cybersecurity experts and took steps to prevent further unauthorized access. We also reported the incident to law enforcement. Although the investigation is ongoing, we have determined that on or about November 16, 2020, an unauthorized third party gained access to Arrow's network and subsequently acquired some of our internal company information from a server before installing the ransomware program. Upon gaining access to the data at issue, Arrow immediately began working with outside experts to determine whether personal information was involved and, if necessary, to be able to carry out the required notifications.

After a detailed search that included a manual review of thousands of files, we recently learned that certain of our customers' personal information was affected. To date, we have identified 3 New Hampshire residents whose personal information was part of the data taken.

The types of personal information affected are the individuals' name and Social Security number. We are not aware of any cases of identity theft or fraud connected to this incident and do not believe the unauthorized third party was targeting personal information in the incident.

Arrow anticipates sending these individuals formal notice on January 8, 2021 via U.S. mail. A sample of the notification letter is enclosed. As stated in the attached sample notice, we are

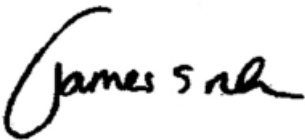
offering to provide individuals 24 months of complimentary identity theft and credit monitoring services through Kroll. We have also established a call center to respond to individuals' questions.

Since discovering the incident, we have taken measures to ensure that the unauthorized third party no longer has access to our systems, and are continuing to monitor and improve our capabilities to detect any further threats and avoid any future unauthorized activity. Specifically, we have replaced all affected computers with either new laptops or new hard drives, deployed additional gatekeeping, monitoring, and screening tools across our IT environment, and organized enhanced e-learning on cybersecurity for Arrow employees, among other measures. Arrow regularly evaluates its security protocols and procedures to ensure that sensitive data is protected as a matter of course. Following the incident, we have also reviewed and reinforced this process to ensure the ongoing security of our systems.

As noted above, our investigation of the incident and our detailed review of the data involved are ongoing, and we anticipate the possibility of additional notifications as we complete this process. We will provide your office with any material updates resulting from this investigation.

Arrow takes the protection of personal information of all of its customers and employees very seriously and is committed to answering any questions that your office may have. Please do not hesitate to contact me at jneu@arrowtruck.com.

Regards,

A handwritten signature in black ink that reads "James Neu". The signature is written in a cursive, flowing style.

James Neu
Executive Vice President & Chief Financial Officer
Arrow Truck Sales, Inc.

Enclosures

January 7, 2021

NOTICE OF SECURITY INCIDENT

Dear [REDACTED],

We are writing regarding a cybersecurity incident that occurred at Arrow Truck Sales, Inc. ("Arrow Truck"). We want to make clear at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred.

WHAT HAPPENED?

On or about November 30, 2020, we learned that an unauthorized third party had gained remote access to Arrow Truck's network in an effort to disrupt our operations. We quickly took steps to secure our network and began to investigate the incident with the support of outside cybersecurity experts. Although the investigation is ongoing, we have determined that the unauthorized third party acquired some of our internal company information, and recently learned that certain of your information was affected.

WHAT INFORMATION WAS INVOLVED?

Based on our review of the materials that were acquired, the personal information acquired by the unauthorized third party included your name and Social Security number.

WHAT WE ARE DOING

We took prompt steps to address this incident, including contacting law enforcement and engaging outside cybersecurity experts to help remediate and ensure the ongoing security of our systems. As part of our ongoing efforts to ensure the security of our systems, we have enhanced cybersecurity protections throughout our environment.

We have also secured the services of Kroll to provide identity monitoring services at no cost to you for two years. Below please find information on signing up for a complimentary two-year membership.

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include one-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 need to activate your membership in order to receive your benefits, and must do so no later than April 8, 2021.

Your Membership Number will not work after this date.

Membership Number: [REDACTED]

Additional information describing your services is included with this letter.

WHAT YOU CAN DO

We strongly encourage you to contact Kroll and take advantage of the identity monitoring services we are providing to you free of charge. Remain vigilant and carefully review your accounts for any suspicious activity.

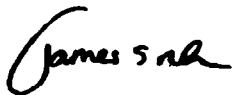
If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or company with which the account is maintained and any relevant government agency, such as IRS, SSA, or state DMV, as applicable.

If you would like to take additional steps to help protect your personal information, attached to this letter are helpful resources on how to do so, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION

We take our responsibility to protect your information extremely seriously, and sincerely regret any inconvenience that this unfortunate incident has caused you. If you have any questions regarding this incident or the services available to you, please contact Kroll at 1-855-526-0331, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your Membership Number ready.

Sincerely,



James Neu
Executive Vice President & Chief Financial Officer
Arrow Truck Sales, Inc.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Additional Resources

Below are additional helpful tips you may want to consider to help protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission (“FTC”) and/or the Attorney General’s office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft. You can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at <https://www.annualcreditreport.com/manualRequestForm.action>. Credit reporting agency contact details are provided below.

Equifax:

equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:

experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:

transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies 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 reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado residents: You may obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, <http://www.marylandattorneygeneral.gov/>, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, <http://www.ncdoj.gov/>, 1-877-566-7226.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, <http://www.ag.ny.gov/home.html>, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, <http://www.dos.ny.gov/consumerprotection>, 1-800-697-1220.
