



Reena R Bajowala
Tel 312.456.1018
reena.bajowala@gtlaw.com

September 20, 2024

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notification of Security Incident

Dear Attorney General Frosh:

We are writing to inform you that our client, CDK Global, LLC, which provides software solutions for the automotive industry ("CDK"), is notifying one (1) individual who resides in Maryland of a data security incident that impacted some of his personal information.

On June 19, 2024, CDK discovered a cyber incident where a third party gained unauthorized access to its systems. Upon learning of the incident, CDK promptly launched an investigation into the matter with the assistance of data forensic experts. Through the investigation, CDK determined that the unauthorized party obtained a copy of files containing certain information relating to current or former vendors of CDK or its corporate predecessor. The information obtained includes name, business or personal address, and business tax identification number or social security number.

CDK takes the security of data it is entrusted with seriously. CDK took immediate steps to contain the incident, and subsequently made enhancements to its systems, security, and practices in collaboration with its third-party data forensic experts. It is working to continuously improve its cybersecurity measures.

Notice to the individual is scheduled to be mailed out today. An example of the notification is attached.

Please contact me for any additional information. Thank you.

Very truly yours,

A handwritten signature in dark ink, appearing to read "Reena R Bajowala".

Reena R Bajowala

GREENBERG TRAURIG, LLP ■ ATTORNEYS AT LAW ■ WWW.GTLAW.COM
77 West Wacker Drive, Suite 3100, Chicago, Illinois 60601 ■ Tel: 312.456.8400 ■ Fax 312.456.8435



CDK Global
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB09357



September 20, 2024

NOTICE OF DATA BREACH

Dear 

CDK Global, LLC is providing notice of a security event that involved some of your information.

What happened? On June 19, 2024, CDK discovered a cyber incident where a third party gained unauthorized access to CDK's systems. Upon learning of the incident, CDK promptly launched an investigation into the matter with the assistance of data forensic experts. The investigation has now concluded. Through the investigation, CDK determined that the third party obtained a copy of certain files containing information relating to vendors of CDK/its corporate predecessor.

Although we have no indication of identity theft or fraud having occurred in relation to this incident, out of an abundance of caution, we are providing you with information about the incident, our response, and additional measures you can take to help protect your information.

What information was involved? Our investigation determined that the following types of information related to you were in the data subject to unauthorized access: Name, business or personal address, and business tax identification number or social security number.

What we are doing. We take the security of data we are entrusted with seriously. Upon discovery of the incident, CDK promptly launched an investigation with the assistance of data forensic experts. CDK notified law enforcement and federal regulators of the incident. This notice has not been delayed by law enforcement. CDK took immediate steps to contain the incident, and has subsequently made enhancements to its systems, security and practices. CDK continuously works to improve its cybersecurity measures.

What you can do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports we are providing (discussed below) for suspicious activity and potential errors, and to report suspected identity theft incidents to local law enforcement or your state's attorney general. Again, CDK is not currently aware of any such incidents relating to the cybersecurity event at issue. Please also review the enclosed *Steps You Can Take to Protect Your Information*, which contains information on what you can do to safeguard against possible misuse of your information.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This

notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **<https://bfs.cyberscout.com/activate>** and follow the instructions provided. When prompted please provide the following unique code to receive services: **5AFF301C598A**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify your information for your own protection to confirm your identity.

What if I want to speak with CDK regarding this incident?

Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

At CDK we take our responsibilities to protect your information seriously. We regret the inconvenience caused by this situation.

Sincerely,

CDK Global, LLC



Steps You Can Take to Protect Your Information

For residents of Maryland: You can obtain information from the Maryland Office of the Attorney General at 200 St. Paul Pl, Baltimore, MD 21202, 1-888-743-0023 <https://www.marylandattorneygeneral.gov/> and the Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338) www.identitytheft.gov about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Massachusetts residents: You have the right to obtain or file a police report.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity and you should immediately report any suspicious activity or incidents of identity theft.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-866-478-0027

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
<http://www.experian.com/freeze/center.html>
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
1-800-916-8800

