UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA

FORMULA SPORTS CARS, INC; PRESTIGE MOTOR CAR IMPORTS, LLC.; BILL HOLT CHEVROLET OF CANTON, INC.; BILL HOLT CHEVROLET OF BLUE RIDGE, INC.; ANNIE ORTIZ; ALEXIS JANET PINO, individually and on behalf of all similarly situated, Plaintiffs, v. CDK GLOBAL, LLC., Defendants.	**CASE NO.: _____** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Formula Sports Cars, Inc.; Prestige Motor Car Imports, LLC.; Bill Holt Chevrolet of Canton, Inc.; Bill Holt Chevrolet of Blue Ridge, Inc.; (collectively, "Dealership Plaintiffs") Annie Ortiz, and Alexis Janet Pino (hereinafter referred to as Consumer Plaintiffs), individually and on behalf of the Classes, defined below, bring this Consolidated Class Action Complaint against defendant CDK Global, LLC ("CDK") for damages, declaratory, injunctive, and other relief. Plaintiffs brings this action against Defendant and allege:

I. INTRODUCTION

1. In the digital age, where cyber threats are increasingly pervasive, the importance of robust cybersecurity measures cannot be overstated. CDK, the largest and most influential software company in the automotive industry, has long touted its commitment to protecting against cyberattacks. In its annual reports, CDK repeatedly emphasizes the critical nature of safeguarding data, stating, "Cybercriminals continue to target dealerships with ever-evolving methods to steal

user and client data, from simply stealing passwords to sophisticated phishing schemes. Protecting your data to avoid IT-related business interruptions, ransom demands, and reputation damage has never been more important. Now is the time to assess and reassess to improve your security and be up to date on the latest cyber threats." CDK Global, *The State of Dealership Cybersecurity 2023*, https://cms.cdkglobal.com/Cybersecurity2023 (last accessed June 23, 2024).

2. Despite these assurances, CDK has failed to uphold its promises and responsibilities that it made throughout the course of its marketing campaigns making users feel at ease they CDK has mastered protecting data it had dominion and control over CDK was fully aware of who was within the zone of risk/harm if the data was compromised to the extent that CDK knew or had foreseeability as it relates to the sensitive information that it stored. This lawsuit addresses CDK's negligence in protecting users of its systems, both businesses and individuals, as well as consumers' data. This negligence has led to significant breaches affecting countless individuals across the United States who have purchased or serviced a vehicle or work at any business location with their personal data stored and accessible within the CDK systems. The repercussions of this failure are far-reaching, exposing sensitive information to cybercriminals and causing irreparable harm to the reputation and trust of the affected parties.

3. CDK's failure to implement adequate security measures, despite its public declarations of vigilance, has resulted in a breach that could have been prevented. This lawsuit seeks to hold CDK accountable for its inability to protect the data entrusted to it by its clients and consumers, underscoring the need for immediate and comprehensive action to rectify these security lapses and prevent future breaches.

4. As stated by an impacted dealership owner "it's a disaster. Customers are coming in, we're selling cars, but we can't book the deals, can't finance the deals or get them to the banks.

Which means we cannot fund the cars or pay off the cars. Manufacturers are shut down because it is affecting the supply chain and service. You cannot process the orders and clearly, you talked about 15,000 dealers affected, there is 17,500 new car dealers, that is 95% . . . . we are losing sales and service . . . ."[1]

5. CDK stands at the heart of the automotive retail industry, with its software systems facilitating 2.6% of the U.S. GDP.[2] As a leading provider of IT and digital solutions, CDK serves over 15,000 dealership operations across North America. Its wide array of services and systems are integral to helping dealerships achieve and enhance customer satisfaction.

6. These systems are crucial to dealerships in order to manage all aspects of dealership operations, from sales, services, parts, inventory, payroll, recalls, and finances. The Dealership Management System ("DMS"), described as a Dealership's "central nervous system," is an enterprise software system designed specifically for automobile Dealerships, and functions as the businesses' central database and repository of all its operational information, including payroll, inventory, human resources, marketing, repair and service, and customer information.

7. The DMS includes a database and data storage component that allows Dealerships to enter and store data in real time.

8. A Dealership's data, stored on its DMS, belongs to and is controlled by the Dealership, which has been explicitly and repeatedly acknowledged in public statements made by Defendant over the years.

[1] Megan Cerullo, *CDK Global Cyber Attack Leaves Thousands of Car Dealerships Spinning Their Wheels*, CBS NEWS (Jun. 24, 2024) https://www.cbsnews.com/amp/news/cdk-cyber-attack-outage-update-2024/

[2] https://www.cdkglobal.com/insights/2023-state-cybersecurity-dealership-study

9. CDK also provides Data Integration Services (DIS), separate from their DMS offerings. DIS services are critical to the proper functioning of Dealerships. DIS enables Dealers and third-party software application providers ("Vendors") to extract, organize, and integrate the Dealer's own data on its DMS into a usable format.

10. This system serves as the backbone of a dealership's day-to-day activities.

II. FACTUAL ALLEGATIONS

11. On June 18, 2024, CDK systems were breached, causing over 15,000 car dealerships to put a halt on key business operations such as sales, financing, and payroll operations (the "CDK Data Breach").

12. Less than 24 hours after the initial breach, CDK began placing their systems back online, only to be subjected to a subsequent breach immediately thereafter. Two major incidents in such a short amount of time raise substantial concerns about the adequacy of CDK's cyber security measures and incident response strategies. CDK's decision to restore their systems without fully resolving the security issues can be likened to a doctor stitching up a wound without first removing all the debris. Just as a wound not properly cleaned would lead to more infections and prolonged healing, CDK's rush to restore its system led to more breaches and, in turn, left car dealerships exposed to financial losses for longer periods of time.

13. As a result, 15,000+ dealerships experienced additional severe disruptions.

14. Critical systems managed by CDK were rendered inoperative.

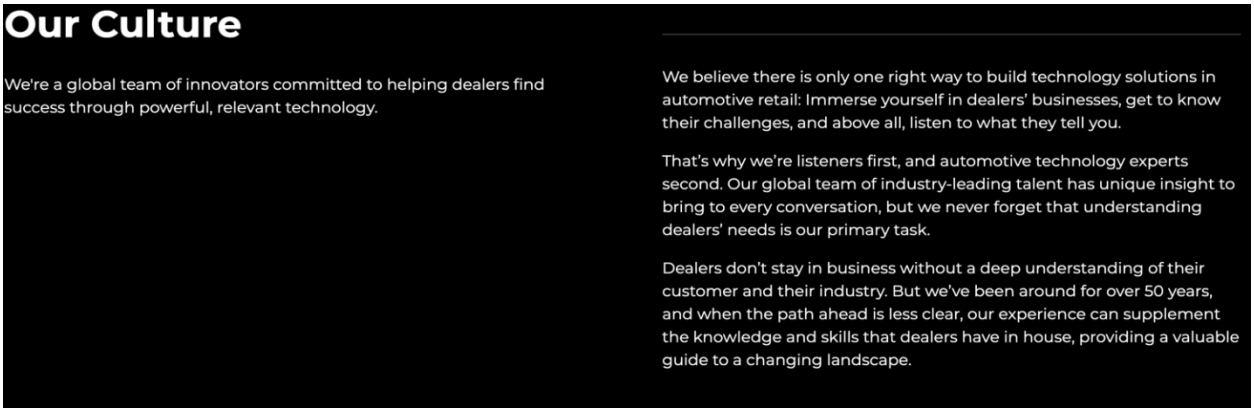
15. Dealerships reverted to manual operations, significantly affecting their ability to effectively conduct business and putting the private information of clients at risk.

16. It is believed that the data breach impacted a combination of information including full name, email addresses, mailing addresses, phone numbers, social security numbers, and dates of birth amongst others.

17. This data breach and the resulting injuries occurred because CDK failed to implement reasonable security procedures and practices (including failing to exercise appropriate managerial control over third-party partner's data security).

18. As a result of CDK's failure to protect the information and systems it was entrusted to safeguard, Plaintiffs and class members' businesses have been irreparably damaged, and its customers and clients now face significant risk of identity theft and fraud, financial fraud, and other identity-relate fraud and into the indefinite future.

19. CDK asserts on its website that its philosophy is that "there is only one right way to build technology solutions in automotive retail: immerse yourself in dealer's business, get to know their challenges, and above all, listen to what they tell you."[3]



Given CDK's self-proclaimed understanding of the automotive retail environment, CDK knew how dependent the Plaintiffs were on their system and knew or should have known of the catastrophic impact one cybersecurity breach could have on the Plaintiff's business, let alone two

[3] CDK Global, *Our Culture*, https://www.cdkglobal.com/about (last accessed June 25, 2024).

cybersecurity breaches in a single week. Instead of ensuring that the issue was fixed and the systems were safe to go back into operation, CDK rushed the process and is now facing ransom from the hackers while CDK's clients suffer the repercussions of their hastiness.

A. *The Breach was Foreseeable and Preventable*

20. At all relevant times, Defendant knew it was storing sensitive personally identifiable information ("PII") and as a result its systems would be attractive targets for cybercriminals.

21. Defendants also knew that a breach of its systems, and exposure of the PII stored within it would result in heightened risk of fraud and identity against those individuals whose PII was exposed.

22. This breach is like many others that come before it; in recent years several high profile breaches have occurred at businesses like Equifax, Yahoo, Marriott, Anthem, amongst others.

23. In 2023, the Federal Trade Commission ("FTC") passed new legislation stating that car dealerships were required to have a comprehensive cybersecurity program in place to comply with the FTC safeguard rule. This new legislation was enacted in response to the rampant increase in cyber-attacks specifically targeting dealerships. Additionally, in 2023 CDK unveiled an 11-page study that they had conducted that highlighted that "Defending against cyber security is more important than ever."[4] The CDK study highlights how cybercriminals are targeting dealerships and the importance of assessing and reassessing to improve one's security measures and to be up to date on the latest cyber threats.

[4] CDK Global, The State of Dealership Cybersecurity 2023, at 3. https://cms.cdkglobal.com/Cybersecurity2023 (last accessed June 23, 2024)

Defending Against Cyberthreats Is More Important Than Ever

Cybercriminals continue to target dealerships with ever-evolving methods to steal user and client data, from simply stealing passwords to sophisticated phishing schemes. Protecting your data to avoid IT-related business interruptions, ransom demands and reputation damage has never been more important. Now is the time to assess and reassess to improve your security and be up to date on the latest cyberthreats.

For this e-book, we compiled data from dealership personnel and market research based on a recent survey conducted by CDK Global. Our goal is to provide dealerships with key insights to consider when evaluating their cybersecurity posture and ongoing strategy.

We've also scattered quotes from dealer participants throughout the book so you can read how other dealers are addressing cybersecurity.

"With all of the manufacturer, customer and our own data stored, it's extremely important to protect it all."

CDK Global, The State of Dealership Cybersecurity 2023, at 3. https://cms.cdkglobal.com/Cybersecurity2023 (last accessed June 23, 2024)

24. The study warns dealerships not to be fooled into thinking it wont happen to their dealership and lays out methods of protection one should follow, which include prevention methods, protection methods, and response methods. Its clear that CDK is very knowledgeable in the world of cyber security and car dealerships and acknowledges the risk given the rampant increase in cyber-attacks towards car dealerships. CDK knew of the importance of safeguarding the system that its clients relied on and knew of the foreseeable consequences that would occur if their systems would need to be shut down, including the financial burden it would place their clients in in the event of a breach. Despite the FTC legislation and their own advisory comments and studies, FTC failed to use reasonable care in safeguarding its system used by the Plaintiff and Class members. Had CDK followed its own advice and adequately invested in data security,

correctly investigated cybersecurity issues, unauthorized parties likely would not have been able to access CDK's systems, and the breach would have been prevented or mitigated accordingly.

B. *Impact of the Breach on Dealership Plaintiffs*

25. Dealership Plaintiffs heavily rely on advanced technological solutions provided by CDK. As found on their company's homepage, CDK represents itself as a global team of innovators committed to helping dealers find success through powerful, relevant technology.[5] These systems are the backbone of the Dealership Plaintiffs' daily operations. Geoff Pohanka, chairman of Pohanka Automotive Group, expressed his frustration with the situation, stating,

> "We are very dependent upon the DMS, and it affects all parts of our business; it generates all of our forms. If you come in, we enter you in the system, it builds a file in terms of paperwork and finance papers. It's debilitating, and the longer it goes on, the harder it will be for dealers."[6]

26. CDK's software facilitates vehicle sales, financing, insurance, repair, and general office operations. The breach came at a time when many car manufacturers began to release new models, and car dealerships across the country advertised promotions on summer deals. Notably, the breach occurred one day before a federal holiday, some of the most profitable days of the year for car dealerships. The system that the Dealership Plaintiffs relied on was compromised, leaving them reverting back to a manual process, using pen and paper to handle sales and customer interactions. This, of course, comes with significant complications and inefficiencies such as increases in time for transactions, prone to errors, and customer dissatisfaction due to extended wait times and being at a competitive disadvantage to those dealerships who did not use CDK's systems.

---

[5] CDK Global, https://www.cdkglobal.com/about (last accessed Jun. 25, 2024).
[6] Megan Cerullo, *CDK Global Cyber Attack Leaves Thousands of Car Dealerships Spinning Their Wheels*, CBS NEWS (Jun. 24, 2024) https://www.cbsnews.com/amp/news/cdk-cyber-attack-outage-update-2024/ .

27. CDK *themselves*, admit that customers do not return to a dealership after they have had a bad experience or their data was compromised.[7]

28. Customers begin to lose trust in the dealerships as personal information gets leaked, such as names, addresses, phone numbers, email addresses, credit scores, and bank account details Contrary to their representations, the recent cybersecurity breach and resulting system outages have clearly demonstrated CDK's failure to provide the "powerful, relevant technology" necessary for dealerships to succeed. CDK's systems have become a vulnerability for these car dealerships by directly undermining dealership operations and causing significant financial loss.

C. <u>Impact of the Breach on Consumer Plaintiffs</u>

29. The link between data breaches and identity theft is clear. Criminals steal personal information to sell on the black market, where it's used for various identity theft crimes.

[7] CDK Global Staff, *Data Privacy What You Should Know*, CDK GLOBAL (Sep. 16, 2022) Khttps://www.cdkglobal.com/insights/data-privacy-what-you-should-know

30. Identity theft becomes easier as more accurate data is obtained. With just a name and birth date, thieves can use social engineering to gather additional details, like login credentials or Social Security numbers, through phishing or spam.

31. The dark web, favored for its anonymity, hosts a sophisticated black market for stolen data, drugs, firearms, and more. Unlike physical goods, digital data can be traded anonymously and instantly. Personal information like Social Security numbers is particularly valuable due to its potential for extensive misuse.

32. Stolen Social Security numbers can lead to significant financial fraud and identity theft, and changing them is difficult. Thieves can use these numbers to open credit accounts, obtain government benefits, file tax returns, and even impersonate victims during arrests.

33. The FBI's 2019 Internet Crime Report highlighted the growing impact of internet-enabled crimes, totaling over $3.5 billion in losses.[8] Rapid reporting can help prevent further fraud, but delays in notification, as seen with some data breaches, exacerbate harm.

34. Victims often face financial losses, emotional stress, and the burden of correcting fraudulent information. The FTC emphasizes the commercial value of consumer data and the need for robust data security practices, including encryption, limited data retention, and monitoring for unauthorized activity.[9]

35. Inadequate breach notifications deprive victims of the chance to protect their information promptly, increasing their risk and harm.

D. <u>Impact of the Breach on Salesperson Plaintiffs</u>

[8] *See 2019 Internet Crime Report Released*, FBI (February 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120

[9] *See Protecting Personal Information: A Guide for Business,* FTC (last accessed June 25, 2024) https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

36. In addition to the operational disruptions experienced by dealerships, commission-based salespersons have suffered significant financial damages due to their inability to complete sales. These individuals, who rely on commission from sales transactions for their income, have been directly impacted by the inability to process and finalize sales, resulting in a substantial loss of earnings.

37. The sales process in automotive dealerships is highly dependent on the functionality of the Dealership Management System (DMS) and Data Integration Services (DIS) provided by CDK. When these systems were compromised, salespersons were unable to access necessary customer information, process financing applications, or complete sales transactions. As a result, potential sales were delayed or lost entirely, directly impacting the commissions these salespersons would have earned.

38. Furthermore, the ongoing uncertainty and reputational damage caused by the breaches have likely resulted in decreased customer traffic and confidence, exacerbating the financial harm to salespersons.

39. Salespersons depend on a steady stream of commissions to cover their living expenses, and the sudden halt in sales has caused severe financial strain. This is a widespread issue affecting numerous salespersons across the 15,000 impacted dealerships.

40. The financial damages suffered by these commission-based salespersons are a direct result of CDK's failure to maintain adequate cybersecurity measures. Their reliance on CDK's systems to perform their job duties underscores the critical nature of these systems to their livelihood. The breaches have not only disrupted dealership operations but have also inflicted personal financial hardship on countless individuals who depend on these commissions to support themselves and their families.

41. Therefore, this lawsuit seeks compensation for the financial losses incurred by commission-based salespersons due to CDK's negligence. These damages include lost commissions, potential future earnings, and the emotional distress caused by the sudden and severe disruption to their income.

42. In sum, CDK's failure to protect its systems has had a cascading effect, extending beyond the dealerships to the individuals whose livelihoods depend on the seamless operation of these systems. It is imperative that CDK is held accountable for the full extent of the damages caused by its security lapses, including the significant financial harm to commission-based salespersons.

III. Jurisdiction and Venue

43. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 putative Class Members, some of which have a different citizenship from the Defendants.

44. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 as all claims alleged herein form part of the same case or controversy.

45. This Court has personal jurisdiction over Defendant CDK Global Inc. as they have engaged in unlawful acts described in this Complaint with the foreseeable or intended effect of causing substantial economic harm to automotive dealers throughout the United States. Defendant has availed itself of the privileges of doing business in Florida through the widespread promotion, sales, marketing, and distribution of their products and services in Florida.

46. The Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b)(2) as a substantial part of the events and omissions giving rise to this action occurred in this District.

Defendant is registered to do business, transacted business, and has agents in this District. A substantial part of the events giving rise to the Plaintiffs' claims arise in this District.

47. Dealership Plaintiff Formula Sports Cars, Inc, is a Florida Corporation, with a principal address at 3800 Bird Rd Coral Gables, FL 33146.

48. Dealership Plaintiff Prestige Motor Car Imports, is a Florida Limited Liability Company, with a principal address at 14800 Biscayne Boulevard, North Miami Beach, FL, 33181

49. Dealership Plaintiff Bill Holt Chevrolet of Canton is a Georgia Corporation, with a principal address at 435 Bethany Green Cove Alpharetta, Georgia 30004.

50. Dealership Plaintiff Bill Holt Chevrolet of Blue Ridge Inc. is a Georgia Corporation, with a principal address at 435 Bethany Cove Alpharetta, Georgia 30004.

51. Dealership Plaintiffs at all relevant times used CDK's systems in the ordinary course of their business.

52. Dealership Plaintiffs rely on CDK's systems to manage vehicle acquisitions, sales, financing, insuring, repairs and maintenance.

53. As a result of the CDK cyber-attack, Dealership Plaintiffs were left with limited to no access to CDK's systems for several days.

54. With limited to no access to CDK's systems, Dealership Plaintiffs have suffered interruptions to their business, loss of sales, and other harm.

55. Plaintiff Annie Ortiz is an individual who at all relevant times has been a citizen and resident of the State of Florida.

56. Plaintiff Alexis Janet Pino is an individual who at all relevant times has been a citizen and resident of the State of Florida.

57. Consumer Plaintiffs purchased a car through a dealership who used the software provided by CDK Global.

58. As a condition of purchasing a vehicle at CDK's clients, Consumer Plaintiffs were required to provide Defendant, directly or indirectly, with their Private Information, including their name, addresses, social security numbers, driver's licenses, and financial details like credit card number and bank account information.

59. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiffs' Private Information in its system.

IV. Class Action Allegations

Plaintiffs bring this action pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) on their own behalf and on behalf of the following Classes:

Nationwide Dealership Class:

> All persons and/or entities utilizing CDK's product(s) in the continental United States and its territories as a software or other operating system as it pertains to any aspect of its business(es), including, but not limited to, management, customer relationships, insurance, operations, sales, services, parts, inventory, marketing, vehicle tracking, payroll, recalls, repairs, registration, workflow and process automation, communication tools, mobile solutions, network and IT solutions, training, support, security and theft prevention, cyber security, telematics and/or financing of vehicles.

Nationwide Consumer Class

> All persons and/or entities who purchased their vehicles at a dealership utilizing CDK's product(s) in the continental United States and its territories as a software or other operating system as it pertains to any aspect of their business(es), including but not limited to, management, customer relationships, insurance, operations, sales, services, parts, inventory, marketing, vehicle tracking, payroll, recalls, repairs, registration, workflow and process automation, communication tools, mobile solutions, network and IT solutions, training, support, security and theft prevention, cyber security, telematics and/or financing of vehicles, and whose personally identifiable information ("PII") was stored in one or more systems or databases of the Defendant whose PII was compromised as a result of the

Defendant's systems being accessed by one or more unauthorized persons or entities as of June 22nd, 2024.

Nationwide Servicer Class:

All persons and/or entities who serviced their vehicles at a dealership utilizing CDK's product(s) in the continental United States and its territories as a software or other operating system as it pertains to any aspect of their business(es), including but not limited to, management, customer relationships, insurance, operations, sales, services, parts, inventory, marketing, vehicle tracking, payroll, recalls, repairs, registration, workflow and process automation, communication tools, mobile solutions, network and IT solutions, training, support, security and theft prevention, cyber security, telematics and/or financing of vehicles, and whose (1) personally identifiable information ("PII") was stored in one or more systems or databases of the Defendant whose PII was compromised as a result of the Defendant's systems being accessed by one or more unauthorized persons or entities as of June 22nd, 2024,and/or (2) experienced delays in the return of their vehicle upon the completion of service.

Nationwide Auto Salesperson Class:

Any commission-based salespersons employed by an auto dealer utilizing CDK's product(s) in the continental United States and its territories as a software or other operating system as it pertains to any aspect of its business(es), including, but not limited to, management, customer relationships, insurance, operations, sales, services, parts, inventory, marketing, vehicle tracking, payroll, recalls, repairs, registration, workflow and process automation, communication tools, mobile solutions, network and IT solutions, training, support, security and theft prevention, cyber security, telematics and/or financing of vehicles.

Nationwide Auto Service Employee Class:

Any service department employee employed by an auto dealer utilizing CDK's product(s) in the continental United States and its territories as a software or other operating system as it pertains to any aspect of its business(es), including, but not limited to, management, customer relationships, insurance, operations, sales, services, parts, inventory, marketing, vehicle tracking, payroll, recalls, repairs, registration, workflow and process automation, communication tools, mobile solutions, network and IT solutions, training, support, security and theft prevention, cyber security, telematics and/or financing of vehicles.

Nationwide Finance Personnel Class:

Any commission-based financing personnel employed by an auto dealer utilizing CDK's product(s) in the continental United States and its territories as a software or other operating system as it pertains to any aspect of its business(es), including,

> but not limited to, management, customer relationships, insurance, operations, sales, services, parts, inventory, marketing, vehicle tracking, payroll, recalls, repairs, registration, workflow and process automation, communication tools, mobile solutions, network and IT solutions, training, support, security and theft prevention, cyber security, telematics and/or financing of vehicles.

60. Excluded from the Classes is Defendant, including any entity or division in which any Defendant has a controlling interest, as well as Defendants' joint ventures, subsidiaries, affiliates, assigns, and successors.

61. The exact number of Class members is unknown to the Plaintiffs. Due to the nature of the trade and commerce involved, Plaintiffs believe there are likely thousands of Class members geographically dispersed throughout the United States, such that joinder of all Class members is impracticable.

62. Class Identity: The members of the Class are readily identifiable and ascertainable. CDK and/or its affiliates, among others, possess the information to identify and contact class members.

63. Numerosity: The members of the Class are so numerous that joinder of all of them is impracticable. CDK itself has stated that there are approximately 15,000 auto dealerships who use the CDK system. Within these systems there are potentially millions who had sensitive PII compromised.

64. Typicality: Plaintiffs' claims are typical of the claims of the members of the Class because all Class members had their PII compromised and/or had suffered interruption to their business as a result of the CDK data breach.

65. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no known interest antagonistic to those of the Class and its interests are aligned with Class members' interests. Plaintiffs were subject to the same data breach as class members,

suffered similar harms, and faces similar threats due to the data breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, involving multiple classes.

66. Commonality and Predominance: There are questions of law and fact common to the Class such that there is a well-defined community of interest in this litigation. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether CDK owed Plaintiffs and Class members a duty to implement and maintain reasonable security procedures and practices to protect their PII;

b. Whether CDK acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;

c. Whether CDK's breach of its duty to exercise due care and conduct reasonable in safeguarding Class members PII directly and/or proximately caused damages to Plaintiffs and Class members;

d. Whether CDK's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class members.

e. Whether CDK adequately addressed and fixed the vulnerabilities that enabled the data breach;

f. Whether Plaintiffs and Class members are entitled to damages to pay for future protective measures like credit monitoring and monitoring for misuse of personal information;

g. Whether Plaintiff and Class members are entitled to damages related to interruptions in its business and lost profits from the CDK data breach.

h. Whether CDK provided timely notice of the data breach to Plaintiffs and Class members; and

i. Whether Class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the data breach.

67. CDK has engaged in a common course of conduct and Plaintiffs and Class members have been similarly impacted by its failure to maintain reasonable security procedures and practices to protect its systems.

68. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences, Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under applicable laws.

V. CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

69. Plaintiffs hereby repeat and realleges paragraphs 1 through 68 of this Complaint and incorporate them by reference herein.

70. Defendant CDK collects Plaintiffs' and Class members' PII in the course of its business. CDK collected and stored this PII for commercial gain. CDK collected, stored, and shared the data to provide its services as well as commercial gain.

71. CDK owed Plaintiffs and Class members, a duty to supervise and ensure its systems maintained adequate data security for the protection of Plaintiffs' and Class members' PII within its control for the purpose of carrying out its business consistent with industry standards. CDK

owed a duty to exercise reasonable care in protecting Plaintiffs' and Class members' PII from unauthorized disclosure or access. CDK acknowledged this duty in its privacy policies describing its handling of PII, where they promised not to disclose PII without authorization.

72. CDK owed a duty of care to Plaintiffs and Class members to provide adequate data security, consistent with industry standards, to ensure that CDK's systems and networks adequately protected the PII.

73. CDK owed a duty of care to Plaintiffs and Class members to remedy any flaws within their system without undue delay so as to alleviate the risk of compromising Plaintiffs' and Class members' PII.

74. CDK's duty to use reasonable care in protecting PII arises because of the parties' relationship, as well as common law and federal law, and CDK's own policies and promises regarding privacy and data security.

75. CDK knew, or should have known, of the risks inherent in collecting and storing PII in a centralized location for the purpose of carrying out its business, vulnerability to network attacks, and the importance of adequate security.

76. CDK breached its duty to Plaintiffs and Class members in numerous ways, as described herein, including by:

a. Failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class members;

b. Failing to ensure that it implemented adequate security systems, protocols, and practices sufficient to protect the PII of Plaintiffs and Class members;

c. Failing to comply with industry standard data security measures for the industry leading up to the Data Breach;

d. Failing to comply with its own privacy policies;

e. Failing to comply with regulations protecting the PII at issue during the period of the data breach;

f. Failing to adequately monitor, evaluate, and ensure the security of their network and systems;

g. Failing to recognize in a timely manner that PII had been compromised; and

h. Failing to timely and adequately disclose the Data Breach.

77. Plaintiffs' and Class members' PII would not have been compromised but for CDK's wrongful and negligent breach of its duties.

78. CDK's failure to take proper security measures to protect the sensitive PII of Plaintiffs and Class members as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access, copying, and exfiltrating of PII by unauthorized third parties.

79. It was also foreseeable that CDK's failure to provide timely and forthright notice of the Data Breach would result in injury to Plaintiffs and Class members.

80. As a direct and proximate result of CDK's conduct, Plaintiffs and Class members have and will suffer damages including: (i) the loss of rental or use value of their PII; (ii) the unconsented disclosure of their PII to unauthorized third parties; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PII; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to,

efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in CDK's possession and is subject to further unauthorized disclosures so long as CDK fails to undertake appropriate and adequate measures to protect it; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives; and (ix) any nominal damages that may be awarded.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

81. Plaintiffs hereby repeat and reallege paragraphs 1 through 68 of this Complaint and incorporate them by reference herein.

82. Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as CDK, of failing to use reasonable measures to protect PII. 15 U.S.C. § 45(a)(1).

83. CDK violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards. CDK's conduct was unreasonable given the nature and amount of PII they obtained, stored, and disseminated in the regular course of their business, and the foreseeable consequences of a data breach, including, specifically, the significant damage that would result to Plaintiffs and Class members.

84. CDK's violations of Section 5 of the FTC Act constitute negligence per se.

85. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

86. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class members. As a direct and proximate result of CDK's negligence *per se,* Plaintiffs and Class members sustained actual losses and damages as alleged herein. Plaintiffs and Class members alternatively seek an award of nominal damages.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

87. Plaintiffs hereby repeat and reallege paragraphs 1 through 68 of this Complaint and incorporate them by reference herein.

88. Plaintiffs and Class members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by CDK and which was stolen in the Data Breach. This information has independent value.

89. Plaintiffs and Class members conferred a monetary benefit on CDK in the form of payments for its services, including those paid indirectly by Plaintiffs and Class members to CDK.

90. CDK appreciated and had knowledge of the benefits conferred upon them by Plaintiffs and Class members.

91. The price for services that Plaintiffs and Class members paid (directly or indirectly) to CDK should have been used by CDK, in part, to pay for the administrative costs of reasonable

data privacy and security practices and procedures, including adequate managerial supervision of vendors' data security.

92. Likewise, in exchange for receiving Plaintiffs' and Class members' valuable PII, which CDK was able to use for its own business purposes and which provided actual value to CDK, CDK was obligated to devote sufficient resources to reasonable data privacy and security practices and procedures, including adequate managerial supervision of vendors' data security.

93. As a result of CDK's conduct, Plaintiffs and Class members suffered actual damages as described herein. Under principles of equity and good conscience, CDK should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds they received from Plaintiffs and Class members, including damages equaling the difference in value between DIS/DMS services that included implementation of reasonable data privacy and security practices that Plaintiffs and Class members paid for and the services without reasonable data privacy and security practices that they actually received.

COUNT IV

BREACH OF FIDUCIARY DUTY
(On Behalf of Purchaser/Servicer Class)

94. Plaintiffs hereby repeat and reallege paragraphs 1 through 68 of this Complaint and incorporate them by reference herein.

95. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

96. As an employee service provider, Defendant has a fiduciary relationship to its clients and their employees, like Plaintiffs and the Class Members.

97. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable Private Information related to Plaintiffs and the Class, which it was required to maintain in confidence.

98. Defendant owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

99. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiffs and the Class members' records.

100. Employees like Plaintiffs and Class members have a privacy interest in personal information, and Defendant had a fiduciary duty not to disclose data concerning its clients' employees.

101. As a result of the parties' relationship, Defendant had possession and knowledge of confidential Private Information of Plaintiffs and Class members, information not generally known.

102. Plaintiffs and Class Members did not consent to nor authorize Defendant to release or disclose their PII to an unknown criminal actor.

103. Defendant breached the duties owed to Plaintiffs and Class Members by, among other things: (a)mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control the employee risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to

adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its patients; and (h) making an unauthorized and unjustified disclosure and release of Plaintiffs and the Class members' PII to a criminal third party.

104. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, their privacy, confidences, and PII would not have been compromised.

105. As a direct and proximate result of Defendant's breach of its fiduciary duties and breach of its confidences, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

i. Loss of their privacy and confidentiality in their PII;

j. The erosion of the essential and confidential relationship between Defendant—as an employee management service provider—and Plaintiffs and Class members as its clients' employees; and Loss of personal time spent carefully reviewing statements from health insurers and providers to check for charges for services not received, as directed to do by Defendant.

106. As a direct and proximate result of Defendant's breach of its fiduciary duty,

107. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiffs and the Class)

108. Plaintiffs hereby repeat and reallege paragraphs 1 through 68 of this Complaint and incorporate them by reference herein.

109. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.,* this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

110. An actual controversy has arisen in the wake of the Data Breach regarding CDK's present and prospective common law and other duties to reasonably safeguard PII and whether CDK is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further cyberattacks and data breaches that could compromise their PII.

111. CDK still possesses PII pertaining to Plaintiffs and Class members and continues to use this PII, which means Plaintiffs' and Class members' PII remains at risk of further breaches because CDK's data security measures remain inadequate. Plaintiffs and Class members continue to suffer injuries as a result of the compromise of their PII and remain at an imminent risk that additional compromises of their PII will occur in the future.

112. Pursuant to the Declaratory Judgment Act, Plaintiffs seeks a declaration that: (a) CDK's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with their obligations and duties of care, (1) CDK must have policies and procedures in place to ensure the parties with whom it shares sensitive personal information maintain reasonable, industry- standard security measures, and must comply with those policies and procedures; (2) Defendants must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class members' PII if it is no longer necessary to perform essential business

functions so that it is not subject to further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

1. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on CDK's systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third- party security auditors;
2. Engaging third-party security auditors and internal personnel to run automated security monitoring;
3. Auditing, testing, and training its security personnel regarding any new or modified procedures;
4. Encrypting PII and segmenting PII by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of its systems;
5. Purging, deleting, and destroying in a reasonable and secure manner PII not necessary to perform essential business functions;
6. Conducting regular database scanning and security checks;
7. Conducting regular employee education regarding best security practices;
8. Implementing multi-factor authentication and POLP to combat system-wide cyberattacks; and
9. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiffs as class representatives and Plaintiffs' counsel as Class Counsel;

B. That the Court grant permanent injunctive relief to prohibit and prevent CDK from continuing to engage in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiffs and Class members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. That the Court award statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law;

E. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by CDK as a result of their unlawful acts, omissions, and practices;

F. That Plaintiffs be granted the declaratory and injunctive relief sought herein;

G. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses; and

H. That the Court award pre-and post-judgment interest at the maximum legal rate and all such other relief as it deems just and proper.

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including, but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

   a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

   b. requiring Defendant to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

   c. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

   d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members; prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

e. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

f. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

g. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures; requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems; requiring Defendant to conduct regular database scanning and securing checks;

h. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

i. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding

subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

m. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

E. For an award of punitive damages, as allowable by law;

F. For an award of attorneys' fees and costs, and any other expenses, including expert witness fees;

G. Pre- and post-judgment interest on any amounts awarded; and

H. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Respectfully submitted,

By: /s/ John H. Ruiz
John H. Ruiz, Esq., Fla. Bar No. 928150

MSP RECOVERY LAW FIRM
2701 S. Lejeune Road, 10th Floor
Coral Gables, FL 33134
Phone: 305-614-2222

John H Ruiz
Fla. Bar No. 928150
jruiz@msprecoverylawfirm.com

Frank Quesada
Fla. Bar No. 29411
fquesada@msprecoverylawfirm.com

Marcus Davide
Fla Bar No. 1025997
mdavide@msprecoverylawfirm.com
serve@msprecoverylawfirm.com

DORTA LAW
334 Minorca Avenue
Coral Gables, FL 33134
Phone: 305-441-2299

Gonzalo Dorta
FL Bar No. 650269
grd@dortalaw.com
file@dortalaw.com

ARMAS BERTRAN ZINCONE
2701 S. LeJeune Rd., 10th Fl.
Miami, FL 33134
Tel: (305) 461-5000

Alfred Armas, Esq.
Fla. Bar No. 360708
alfred@armaslaw.com

Francesco A. Zincone, Esq.
Fla. Bar No. 100096
fzincone@armaslaw.com

Eduardo E. Bertran, Esq.
Fla. Bar No. 94078
ebertran@armaslaw.com