IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

RONALDO PROTO, individually and on behalf of all others similarly situated, Plaintiff, v. CDK GLOBAL, LLC, Defendant.	Case No. 1:24-cv-6168 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Ronaldo Proto ("Plaintiff") brings this Class Action Complaint on behalf himself, and all others similarly situated, against Defendant CDK Global, LLC ("CDK" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE ACTION

1. Companies that handle, collect, and store sensitive, personally identifying information ("PII") owe a duty to the individuals to whom that data relates. This duty arises because it is foreseeable that the exposure of PII to unauthorized persons—and especially hackers with nefarious intentions—will result in harm to the affected individuals, including, but not limited to, identity theft and fraud.

2. CDK is a software-as-a-service ("SaaS") provider, that provides automotive dealers with a software platform to run all aspects of their operations, including sales, financing, inventory,

service, and back office functions.[1] CDK's platform is widely used, serving over 15,000 car dealerships in North America.[2]

3. In the course of providing its SaaS platform to its dealership customers, CDK is entrusted with a wide variety of PII, including dealerships' customer information, including, but not limited to names, contact information, Social Security numbers, employment history, and proof of income.

4. By knowingly collecting and storing individuals' PII, CDK has a resulting duty to implement and maintain reasonable data security measures to protect such information from unauthorized access and exfiltration.

5. CDK expressly recognizes this duty, representing that "[c]ybersecurity is a business priority" and further representing that CDK provides its dealership customers with "triple-layer security" that provides dealerships with "peace-of-mind previously known only to large corporations with expensive in-house cybersecurity personnel."[3]

6. CDK's cybersecurity promises nevertheless fell flat beginning June 19, 2024 when a cyber-attack prompted Defendant to shutdown most of it systems "out of an abundance of caution." While CDK attempted to restore some of its systems later that day, Defendant suffered a second cyber-attack, prompting Defendant to take its systems offline again.[4] The sequence of

---

[1] Lawrence Abrams, *CDK Global outage caused by BlackSuit ransomware attack*, BleepingComputer (June 22, 2024), https://www.bleepingcomputer.com/news/security/cdk-global-outage-caused-by-blacksuit-ransomware-attack/.

[2] Lawrence Abrams, *CDK Global cyberattack impacts thousands of US car dealerships*, BleepingComputer (June 19, 2024), https://www.bleepingcomputer.com/news/security/cdk-global-cyberattack-impacts-thousands-of-us-car-dealerships/.

[3] *Dealership Security*, CDK, https://www.cdkglobal.com/dealership-operations/cybersecurity (last visited July 22, 2024); *CDK Security Suite*, CDK, https://www2.cdkglobal.com/network-cdk-security-suite (last visited July 22, 2024).

[4] Mary Walrath-Holdridge, Kinsey Crowley, & Bailey Schultz, *CDK Global cyberattack: See timeline of the hack, outages and when services could return*, USA Today (July 3, 2024),

cyber-attacks resulted in a two-week disruption to Defendant's SaaS platform, crippling the automotive industry, leaving many dealerships unable to perform daily operations, and forcing some to resort to manual processes or otherwise halt activities entirely (the "Data Breach").[5]

7. Upon information and belief, the threat actors responsible for the Data Breach were able to access and exfiltrate sensitive PII relating to dealerships' customers stored in CDK's SaaS platform.

8. As a direct and proximate result of CDK's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII—names, contact information, Social Security numbers, employment history, and proof of income—is now in the hands of cybercriminals.

9. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, and other harms caused by the unauthorized disclosure of their PII—risks which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

10. As such, on behalf of themselves and all others similarly situated, Plaintiff brings claim for negligence, negligence *per se*, unjust enrichment, and declaratory judgment, seeking damages and injunctive relief, including the adoption of reasonably sufficient data security practices to safeguard the PII in Defendant's possession in order to prevent incidents like the Data Breach from reoccurring in the future.

---

https://www.usatoday.com/story/money/2024/07/03/cdk-global-cyberattack-timeline/74292877007/.

[5] Samantha Delouya, *'I can't get paid.' Cyberattack affecting car dealerships brings chasos for sellers, buyers, and workers*, CNN (June 30, 2024), https://www.cnn.com/2024/06/30/cars/cdk-outage-car-dealers/index.html.

PARTIES

11. Plaintiff Ronald Proto is an adult who, at all relevant times, is and was a citizen of the State of Connecticut.

12. Defendant CDK is a Delaware limited liability company with a principal place of business located at 1950 Hassell Road, Hoffman Estates, Illinois 60169.

13. Upon information and belief, CDK is a single member limited liability company with its sole member being CDK Global Holdings II, LLC. CDK Global Holdings II, LLC is a single member limited liability company with its sole member being CDK Global Holdings, LLC. CDK Global Holdings, LLC is a single member limited liability company with its sole member being CDK Global II, LLC. CDK Global II, LLC is a single member limited liability company with its sole member being Central Parent LLC. Central Parent LLC is a single member limited liability company with its sole member being Central HoldCo LLC. Central HoldCo LLC is a single member limited liability company with its sole member being Central TopCo, Inc., a Delaware corporation.

14. Defendant CDK is a citizen of the states in which its member is a citizen. CDK is a citizen of the State of Delaware.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because Plaintiff and at least one member of the Class, as defined below, are citizens of a different state than Defendant, there are more than 100 members of each of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

16. This Court has general personal jurisdiction over Defendant because CDK resides in State of Illinois.

17. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(b)(1), because Defendant resides in this District, a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this District; and Defendant conducts substantial business within this District.

FACTUAL BACKGROUND

A. CDK Collects and Stores Plaintiff's and Class Members' PII.

18. CDK provides its clients in the automative industry with a SaaS platform to run all aspects of their operations, including sales, financing, inventory, service, and back office functions.

19. CDK purports to be "at the epicenter of automotive retail" representing that 2.6 percent of the United States' Gross Domestic Product is transacted through CDK Global.[6]

20. Part of CDK's SaaS platform includes its Dealer Management System ("DMS"), which CDK represents as a "suit of powerful software tools that equips auto dealers with solutions they need to be profitable on one fully integrated platform."[7]

21. In the course of providing its DMS to its dealership customers, CDK is entrusted with a wide variety of Plaintiff's and Class Members' PII, including names, contact information, Social Security numbers, employment history, and proof of income.

22. CDK recognizes that by collecting and storing customer PII, Defendant is responsible for keeping this information confidential and secure, representing that "cybersecurity is a business priority" and further representing that Defendant provides a "three-tiered

[6] *Dealer Management System*, CDK, https://www.cdkglobal.com/dms (last visited July 22, 2024).
[7] *Id.*

cybersecurity strategy to prevent, protect and respond to cyberattacks so you can defend your dealership."[8]

23. CDK also represents that a key function of its DMS is ensuring Federal Trade Commission compliance, helping dealerships to "protect [themselves], minimize fraud and detect irregularities with solutions that help [then] comply with the FTC Safeguards Rule."[9]

24. Aware of how important data security is to both dealerships and their customers, a CDK research paper identified cyber threats as a top priority for dealers and further recognized that dealerships are routinely targeted by cyber-attacks, with seventeen percent of respondents to a survey indicating that they had suffered a cyber-attack or incident within the past year.[10] Indeed, in another paper, CDK recognizes that cybersecurity is essential to dealerships, stating that "[f]rom ransomware to data breaches, dealerships are under attack at unprecedent levels and protecting your data has never been more important."[11]

25. Despite representing that its SaaS platform is a solution to the problem of data security, however, CDK's representations fell flat.

B. The Data Breach.

26. On or about June 19, 2024, a cyber-attack prompted Defendant to shutdown most of its systems "out of an abundance of caution." While CDK attempted to restore some of its systems later that day, Defendant suffered a second cyber-attack, prompting Defendant to take its

[8] *Dealership Security*, *supra* note 3.
[9] *Dealer Management System*, *supra* note 6.
[10] *The State of Dealership Cybersecurity 2023*, CDK Global (2023), https://cms.cdkglobal.com/Cybersecurity2023.
[11] *FTC Safeguards Rule: A Guide for Car Dealerships*, CDK (202), https://www.cdkglobal.com/sites/cdk4/files/2022-12/22-8350%20FTC%20Safeguards%20Guide%20for%20Dealers%20Ebook_v9_dec16-22.pdf.

systems offline again.[12] The sequence of cyber-attacks resulted in a two-week disruption to Defendant's SaaS platform.[13]

27. On or about June 22, 2024, new outlets began reporting that outage to Defendant's SaaS platform was really a ransomware attack and that CDK had been in negotiations with the ransomware group responsible in order to receive a decryptor and prevent any stolen data from being leaked.[14]

28. As such, it appears that the Data Breach was a targeted attack that resulted in the successful encryption of Defendant's computer systems and the unauthorized access to and theft of data from such systems. Indeed, Cybersecurity experts warn that "[m]ost if not all, ransomware incidents will involve the theft of data from a victim's network. When a cybercriminal deploys ransomware, it should be assumed that data has been stolen."[15]

29. In conjunction with cybersecurity experts' warnings about ransomware attacks, following the Data Breach, numerous news articles warned that those who recently purchased or leased a vehicle from a dealership using CDK's platform should assume their PII, including names, addresses, Social Security numbers, employment histories, and proof of income had been compromised in the Data Breach.[16]

---

[12] Walrath-Holdridge, *et. al.*, *supra* note 4.
[13] *Id.*
[14] Abrams, *supra* note 1.
[15] Cyber Crime Assessments Team, *What's Happened to my data?*, National Cyber Security Centre (May 9, 2024), https://www.ncsc.gov.uk/blog-post/whats-happened-data#:~:text=No%20longer%20'just%20encryption',that%20data%20has%20been%20stolen.
[16] Jennifer Gregory, *Hackers are increasingly targeting auto dealers*, Security Intelligence (July 11, 2024), https://securityintelligence.com/news/hackers-increasingly-targeting-auto-dealers/; Wyatte Grantham-Philips, *Car dealerships in North America revert to pens and paper after cyberattacks on software provider*, KRGV (June 24, 2024), https://www.krgv.com/news/car-dealerships-in-north-america-revert-to-pens-and-paper-after-cyberattacks-on-software-provider/.

30. Following the Data Breach, CDK purportedly took steps to contain the incident, including paying a $25 million ransom to the ransomware group responsible for the Data Breach.[17] But even if Defendant took steps end the prolonged outage and ensure the deletion of any stolen data, *i.e.*, paid the threat actors a ransom to ensure the stolen information's destruction, criminals have no incentive to destroy such valuable information that may be monetized in the future, either through extracting additional ransom payments (from CDK), or using the data to commit fraud and identity theft. As cybersecurity professional Brian Krebs has noted:

> Companies hit by ransomware often face a dual threat: Even if they avoid paying the ransom and can restore things from scratch, about half the time the attackers also threaten to release sensitive stolen data unless the victim pays for a promise to have the data deleted. Leaving aside the notion that victims might have any real expectation the attackers will actually destroy the stolen data, new research suggests a fair number of victims who do pay up may see some or all of the stolen data published anyway.[18]

31. Indeed, law enforcement action against certain ransomware gangs has revelated that data from victims who paid the ransom was still on the gang's systems, highlighting that a victim can never be sure that all the stolen data has been deleted, even if they pay the ransom.[19]

32. Following CDK's ransom payment, Defendant began bringing car dealers back online to its SaaS platform, ending the prolonged outage.[20]

33. Upon information and belief, the Data Breach is the direct and proximate result of CDK's failure to implement adequate data security measures.

---

[17] Sean Lyngaas, *How did the auto dealer outage end? CDK almost certainly paid a $25 million ransom*, CNN (July 11, 2024), https://www.cnn.com/2024/07/11/business/cdk-hack-ransom-tweny-five-million-dollars/index.html.
[18] Brian Krebs, *Why Paying to Delete Stolen Data is Bonkers*, Krebs on Security (Nov. 20, 2020), https://krebsonsecurity.com/2020/11/why-paying-to-delete-stolen-data-is-bonkers/.
[19] Cyber Crime Assessments Team, *supra* note 15.
[20] Lyngaas, *supra* note 17.

C. The Value of Private Information and the Effects of Unauthorized Disclosure.

34. CDK was well aware that the highly sensitive PII which it acquires is highly sensitive and of significant value to those who would use it for wrongful, nefarious purposes.

35. CDK also knew that a breach of its computer systems, and exposure of the PII therein, would result in the increased risk of identity theft and fraud against the individuals whose PII was compromised.

36. These risks are not theoretical, numerous high-profile breaches have occurred at third-party service providers, such as Progress Software, Fortra, and Accellion in recent years.

37. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[21] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

38. Criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

39. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities. In 2023, there were 3,205 publicly disclosed data compromises, affecting

[21] *What To Know About Identity Theft*, FED. TRADE COMM'N CONSUMER ADVICE (Apr. 2021), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited July 22, 2024).

over 353 million victims. The U.S. specifically saw a 72% increase in data breaches from the previous all-time high in 2021 and a 78% increase over 2022.[22]

40. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased in recent years. For instance, in 2019, roughly 3.5 million people reported some form of identity theft, fraud, or other consumer complaint compared to 5.4 million people in 2023.[23]

41. CDK's own research recognizes that auto dealerships are increasingly concerned with cybersecurity in the face of an alarming rise in cyber-attacks. Indeed, CDK's research reveals that while ninety percent of dealerships are concerned about cybersecurity and fifty-three percent of dealers being confident about their current cybersecurity protections, seventeen percent of dealerships experienced a cyberattack or incident in 2023.[24]

42. Automotive dealers have become an attractive target in part because the data they possess represents a "treasure of information," including large amounts of personal data related to financial and credit applications, customer financial information, and home addresses.[25]

---

[22] *2023 Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

[23] *Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Key%20Facts (last visited July 22, 2024).

[24] *Driving Into Danger: CDK Global 2023 Cybersecurity Report Reveals Rise in Auto Dealership Cyberattacks*, CDK (Oct. 23, 2023), https://www.cdkglobal.com/media-center/driving-danger-cdk-global-2023-cybersecurity-report-reveals-rise-auto-dealership.

[25] *Acting with urgency against the cyber threats to auto dealers*, Zurich, https://www.zurichna.com/-/media/project/zwp/zna/knowledge/docs/acting-with-urgency-against-cyber-threats.pdf (last visited July 22, 2024).

43. The breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and Class Members especially vulnerable to identity theft, tax fraud, credit and bank fraud, and more.

44. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique social security numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

45. The Social Security Administration even warns that the process of replacing a Social Security number is a difficult one that creates other types of problems, and that it will not be a panacea for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[26]

[26] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf.

46. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

47. The ramifications of CDK's failure to keep Plaintiff's and Class Members' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

48. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[27]

49. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Indeed, even where cybercriminals do not gain access to a complete set of an individual's PII during a data breach, cybercriminals can cross-reference two or more sources of PII to marry data available elsewhere with criminally stolen data, resulting in complete and accurate dossiers on individuals. These dossiers are known as "Fullz" packages.

[27] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited July 22, 2024).

50. The development of Fullz packages means stolen PII from a data breach can easily be linked to victims' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information (such as emails, phone numbers, or credit card numbers) is not included in the PII stolen in a specific incident, criminals can easily create a Fullz package that links that information together and sell the package at a higher price.

51. Importantly, once a cybercriminal has a Fullz package, they can use it to commit a host of criminal acts including: credit card fraud, loan fraud, identity fraud, account take overs, medical identity fraud, tax refund fraud, and buy now pay later frauds.[28] Most problematic, however, is that cybercriminals in possession of a Fullz package "are difficult to stop with ordinary online security and ID verification measures because they possess all the information needed to get past typical authentication measures."[29]

52. A poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[30]

53. As a technology company that deals exclusively in data storage and processing, CDK was uniquely positioned to ensure the safety of the PII stored on its platform.

54. CDK also knew or should have known the importance of safeguarding the PII stored on its platform and of the foreseeable consequences if its data security systems were

---

[28] Paige Tester, *What Are Fullz? How Hackers and Fraudsters Obtain and Use Fullz*, DATADOME (Mar. 3, 2024), https://datadome.co/guides/account-takeover/what-are-fullz-how-do-fullz-work/.

[29] *Protection Against Fullz and Fraud*, INTEGRITY (Apr. 18, 2022), https://integrity.aristotle.com/2022/04/protection-against-fullz-and-fraud/.

[30] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864.

breached. CDK failed, however, to take adequate cybersecurity measures to prevent the Data Breach exfiltration of Plaintiff's and Class Members' PII from occurring.

D. CDK Failed to Comply with FTC Guidelines and Industry Best Practices.

55. CDK is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

56. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[31]

57. The FTC recommends that businesses:[32]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should

[31] *Start with Security: A Guide for Business*, U.S. Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 22, 2024).

[32] *Protecting Personal Information: A Guide for Business*, U.S. Federal Trade Comm'n (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited July 22, 2024).

be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

58. The FTC further recommends business take additional cybersecurity steps, which include:[33]

a. Conducting an inventory of all company devices that store sensitive data, and understanding what types of PII is stored on those devices;

b. Encrypting sensitive personal information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

c. Crafting a data security plan that involves both physical security (*e.g.*, locking up physical files) and electronic security, and training employees regarding the data security plan.

d. Promptly disposing of PII that is no longer needed, and retaining sensitive data only as long as companies maintain a legitimate business need for the information; and

e. Developing a plan to handle a data breach or data security incident, if and when such an incident occurs.

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[33] *Id.*

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Upon information and belief, CDK failed to properly implement one or more of the basic data security practices described above. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII resulted in the unauthorized access to and exfiltration of Plaintiff's and Class Members' PII. CDK's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

61. Similarly, the U.S. Government's National Institute of Standards and Technology ("NIST") provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[34]

62. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[35] Upon information and belief, CDK failed to adhere to the NIST guidance.

63. Further, the National Automobile Dealers Associations recommends that that dealers implement the following data security requirements to comply with their requirements under the FTC's safeguard rule, including:[36]

---

[34] *See Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[35] *Id.* at Table 2 pg. 26-43.
[36] *FTC Safeguards Rule*, Nat'l Automobile Dealers Ass'n, https://www.nada.org/safeguardsrule (last visited July 22, 2024).

a. Designating a qualified individual to oversee their information security program;

b. Developing a written risk assessment;

c. Limiting and monitoring who can access sensitive customer information;

d. Encrypting all sensitive information;

e. Training security personnel;

f. Developing an incident response plan;

g. Periodically assessing the security practices of service providers; and

h. Implementing multi-factor authentication or another method with equivalent protection for any individual accessing customer information.

64. Upon information and belief, Defendant's failure to protect Plaintiff's and Class Members' PII is a result of CDK's failure to adopt reasonable safeguards as required by the FTC, NIST, and industry best practices.

65. CDK was, at all times, fully aware of its obligations to protect the PII of consumers because of its business model of collecting PII to provide its SaaS platform to its dealership customers. CDK were also aware of the significant repercussions that would result from its failure to do so.

E. Plaintiff and Class Members Suffered Damages.

66. The ramifications of CDK's failure to keep consumers' PII secure are long-lasting and severe. Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways, including theft of their PII as well as substantial and imminent risk of identity theft and fraud. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit

and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering, spear phishing, or extortion attacks; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

67. In 2019, the United States Government Accountability Office ("GAO") released a report addressing the steps consumers can take after a data breach.[37] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. It is clear from the GAO's recommendations that the steps data breach victims (like Plaintiff and Class Members) must take after a data breach, like Defendant, are both time-consuming and of only limited and short-term effectiveness.

68. The FTC, like the GAO, recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[38]

69. Further, once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse.

---

[37] Government Accountability Off., *Data Breaches* (Mar. 2019) https://www.gao.gov/assets/gao-19-230.pdf (last visited July 22, 2024).

[38] *See Identity Theft Victim Checklist*, Fed. Trade Comm'n, https://www.identitytheft.gov/Steps (last accessed July 22, 2024).

70. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when PIIs stolen and when it is used. According to the GAO, which has conducted studies regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[39]

71. For these reasons, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

72. The value of Plaintiff's and Class Members' PII has been diminished by its exposure in the Data Breach. Indeed, PII is a valuable commodity to identity thieves, and, once it has been compromised, criminals will use them and trade the information on the cyber black market for years thereafter.[40]

73. The reality is that cybercriminals seek nefarious outcomes from a data breach, and stolen PII can be used to carry out a variety of crimes.

74. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' PII.

75. As a result of CDK's failures, Plaintiff and Class Members face an increased risk of identity theft and fraud, phishing attacks, and related cybercrimes because of the Data Breach.

---

[39] *See* 2007 GAO Report, at 29.

[40] *The Price Cybercriminals Charge for Stolen Data*, Trustwave (Aug. 6, 2023), https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/the-price-cybercriminals-charge-for-stolen-data/.

Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk of falling victim to cybercrimes for years to come.

76. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers and cybercriminals.

F. Plaintiff's Experience.

77. Plaintiff leased a vehicle earlier this year from his local Hyundai dealer, who, upon information and belief, uses CDK software to facilitate vehicle sales and financing.

78. In order to lease a vehicle from his local Hyundai dealership, Plaintiff was required to entrust his PII, including his name, contact information, Social Security number, employment history, and proof of income to his local Hyundai dealership. Plaintiff's PII was ultimately collected and stored by CDK.

79. On or about June 2024, Plaintiff was notified that his PII may have been compromised in the Data Breach.

80. Since the Data Breach, Plaintiff has been required to spend his valuable time and effort taking steps to mitigate the risk of misuse of his PII. Specifically, Plaintiff has been required to spend his valuable time and effort reviewing his credit report for suspicious activity, calling his bank to ensure there has been no suspicious activity on his accounts, and calling his bank to set up alerts if any money is withdrawn from his account. Plaintiff would not have had to engage in these time intensive efforts but for the Data Breach.

81. Plaintiff has suffered actual injury from having his PII exposed and/or stolen as a result of the Data Breach, including: (a) mitigation efforts to prevent the misuse of his PII; (b) damages to and diminution of the value of his PII, a form of intangible property that loses value

when it falls into the hands of criminals who are using that information for fraud or publishing the information for sale on the dark web; and (c) loss of privacy.

82. Given the nature of the information compromised in the Data Breach and the propensity of criminals to use such information to commit a wide variety of financial crimes, Plaintiff faces a significant, present, and ongoing risk of identity theft and fraud, and other identity-related fraud now and into the indefinite future.

83. In addition, knowing that hackers accessed and likely exfiltrated his PII and that this information likely has been and will be used in the future for identity theft, fraud, and other nefarious purposes has caused Plaintiff to experience significant frustration, anxiety, worry, stress, and fear.

CLASS ACTION ALLEGATIONS

84. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States whose PII was compromised in the CDK Data Breach that began on or about June 19, 2024.

85. Excluded from the Class is Defendant, its subsidiaries and affiliates, its officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

86. Plaintiff reserves the right to modify or amend the definition of the proposed Class prior to moving for class certification.

87. **Numerosity.** The members of the Class are so numerous that the joinder of all members is impractical. Plaintiff is informed and believes, and thereon alleges, that there are at

least thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach.

88. **Commonality.** This action involves questions of law and fact that are common to Plaintiff and the Class members. Such common questions include, but are not limited to:

a. whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class members;

b. whether Defendant was negligent in collecting and storing Plaintiff's and Class members' PII;

c. whether Defendant had duties not to disclose the PII of Plaintiff and Class members to unauthorized third parties;

d. whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class members' PII;

e. whether Defendant failed to adequately safeguard the PII of Plaintiff and Class members;

f. whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class members' PII;

g. whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. whether Plaintiff and Class members are entitled to damages as a result of Defendant's wrongful conduct; and

i. whether Plaintiff and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

89. **Typicality.** Plaintiff's claims are typical of the claims of the Class members. The claims of Plaintiff and Class members are based on the same legal theories and arise from the same failure by Defendant to safeguard their PII. Plaintiff and Class members directly and/or indirectly entrusted Defendant with their PII, and it was subsequently released to an unauthorized third party.

90. **Adequacy of Representation.** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

91. **Superiority.** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

92. **Predominance.** Common questions of law and fact predominate over any questions affecting only individual Class members. Similar or identical violations, business

practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages is common to Plaintiff and each member of the Class. If Defendant breached its duty and released Plaintiff's and Class Members' PII, then Plaintiff and each Class member suffered damages by that conduct.

93. **Ascertainability.** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class members may be readily identified through Defendant's books and records.

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

94. Plaintiff restates and realleges all proceeding allegations as if fully set forth herein.

95. CDK owed a duty under common law to Plaintiff and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting their PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

96. Specifically, this duty included, *inter alia*: (a) designing, maintaining, and testing CDK's security systems to ensure that Plaintiff's and Class members' PII in CDK's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

97. CDK's duty to use reasonable care arose from several sources, including but not limited to those described below.

98. CDK had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By storing and processing valuable PII that is routinely targeted by cybercriminals, CDK was obligated to act with reasonable care to protect against these foreseeable threats.

99. Defendant also owed a common law duty because its conduct created a foreseeable risk of harm to Plaintiff and Class Members. CDK's conduct included its failure to adequately restrict access to its computer networks, servers, and/or cloud computing accounts that held individuals' PII.

100. CDK also knew or should have known of the inherent risk in collecting and storing massive amounts of PII, the importance of implementing adequate data security measures to protect that PII, and the frequency of cyberattacks such as the Data Breach that target third-party service providers.

101. CDK breached the duties owed to Plaintiff and Class members and thus was negligent. CDK breached these duties 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 customer information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these 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 their 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 own privacy policies provided to

customers; and (h) failing to adequately train and supervise employees access or credentials to systems and databases containing sensitive PII.

102. But for CDK's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their PII would not have been compromised.

103. As a direct and proximate result of CDK's negligence, Plaintiff and Class members have suffered injuries including:

a. theft of their PII;

b. unauthorized charges to their bank accounts;

c. costs associated with canceling and ordering new payment cards;

d. time spent reporting fraudulent activity;

e. costs associated with requesting credit freezes;

f. costs associated with the detection and prevention of identity theft;

g. costs associated with purchasing credit monitoring and identity theft protection services;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. 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 Data Breach;

j. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

k. damages to and diminution in value of their PII entrusted to CDK with the mutual understanding that Defendant would safeguard Plaintiff's and Class

members' data against theft and not allow access and misuse of their data by others; and

l. continued risk of exposure to hackers and thieves of their PII, which remains in CDK's possession and is subject to further breaches so long as CDK fails to undertake appropriate and adequate measures to protect Plaintiff and Class members.

104. As a direct and proximate result of CDK's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

105. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

106. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as CDK of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

107. CDK violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature of its business and the amount of PII it obtained and stored. CDK was perhaps most aware of the foreseeable consequences of a data breach.

108. CDK's violation of Section 5 of the FTC Act constitutes negligence *per se*.

109. Plaintiff and Class members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

110. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. The FTC has pursued over fifty 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 suffered by Plaintiff and Class members.

111. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including those identified in paragraph 110 above.

112. As a direct and proximate result of CDK's negligence, Plaintiff and Class members have been injured as described herein and above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

113. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

114. Plaintiff and Class members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by CDK and that was ultimately accessed or compromised in the Data Breach.

115. Plaintiff and Class members conferred a monetary benefit upon CDK in the form of monies paid to Defendant's dealership customers for services and/or products. CDK's business model would not exist save for the need to ensure the security of Plaintiff's and Class members' PII in order to provide its SaaS platform to its customers.

116. The relationship between CDK and Plaintiff and Class members is not attenuated, as Plaintiff and Class members had a reasonable expectation that the security of their PII would be maintained when they provided their information to CDK's dealership customers.

117. By engaging in the conduct described in this Complaint, CDK has knowingly obtained and derived benefits from Plaintiff and Class members at Plaintiff's and Class members' expense, namely the profits gained in exchange for the use of CDK's services, such that it would be inequitable and unjust for Defendant to retain them.

118. By engaging in the acts and failures to act described in this Complaint, CDK has been knowingly enriched by the financial gain. This profit should have been reasonably expended to protect the PII of Plaintiff and the Class. Defendant knew or should that known that theft of consumer PII was a constant threat, yet it failed to take reasonable steps to ensure the level of security required to have prevent the theft of consumers PII.

119. CDK's failure to direct profits derived from Plaintiff's and Class members' patronage of its customers toward safeguarding Plaintiff's and Class members' PII constitutes the inequitable retention of a benefit without payment for its value.

120. CDK will be unjustly enriched if it is permitted to retain these benefits following the theft of Plaintiff's and Class members' PII.

121. CDK's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and inadequate security of Plaintiff's and Class members' PII, while at the same time failing to securely maintain that information from unauthorized access and compromise.

122. Plaintiff and Class members have no adequate remedy at law.

123. As a direct and proximate result of CDK's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, including those identified in paragraph 103 above.

124. CDK should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

125. Plaintiff restates and realleges all proceeding factual allegations as if fully set forth herein.

126. 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 to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described herein.

127. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class members' PII and whether CDK is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Defendant still possess Plaintiff's and Class members' PII, and that Defendant's data security measures remain inadequate. Furthermore, Plaintiff and Class members continue to suffer injury as a result of the compromise of their PII and remains at imminent risk that further compromises of their PII will occur in the future.

128. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. CDK owes a legal duty to secure consumers' PII under the common law and Section 5 of the FTC Act; and

b. CDK continues to breach this legal duty by failing to employ reasonable data security measures to safeguard Plaintiff's and Class members' PII.

129. This Court also should issue corresponding prospective injunctive relief requiring CDK to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

130. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at CDK. The risk of another such breach is real, immediate, and substantial. If another breach of CDK's SaaS platform occurs, Plaintiff and Class members will not have an adequate remedy at law because the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

131. The hardship to Plaintiff and Class members if an injunction is not issued exceeds the hardship to CDK if an injunction is issued. Plaintiff and Class members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to CDK of complying with an injunction by employing reasonable prospective data security measures is relatively minimal. CDK has a pre-existing legal obligation to employ such measures.

132. Issuance of the requested injunction will not disserve the public interest. On the contrary, such an injunction would benefit the public by possibly preventing another data breach at CDK, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, prays for relief as follows:

A. for an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

B. for an order finding in favor of Plaintiff and the Class on all counts asserted herein;

C. for damages in an amount to be determined by the trier of fact;

D. for an order of restitution and all other forms of equitable monetary relief;

E. declaratory and injunctive relief as described herein;

F. awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

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

H. awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded on all claims so triable.

Dated: July 22, 2024

Respectfully submitted,

/s/ Katrina Carroll
Katrina Carroll
LYNCH CARPENTER, LLP
111 W. Washington St.
Suite 1240
Chicago IL 60602
T: (312) 750-1265
katrina@lcllp.com

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
T: (412) 322-9243
gary@lcllp.com

Attorneys for Plaintiff and the Proposed Class