IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

MICHAEL MARTINEZ, individually, and on behalf of all others similarly situated, Plaintiff, v. KOHL'S, INC., Defendant.	Case No. 24-5405 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Michael Martinez, individually, and on behalf of all similarly situated persons, alleges the following against Defendant Kohl's Inc. ("Defendant" or "Kohl's"), based on personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by his counsel and review of public documents, as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff's and other similarly situated customers' ("Class Members," as defined *infra*) sensitive personally identifiable information, including their names, Social Security numbers, dates of birth, and account information ("PII").

2. Financial Business and Consumer Solutions, Inc. ("FBCS") is a nationally licensed debt collection agency in the United States, specializing in collecting unpaid debts from consumer credit, healthcare, commercial, auto loans and leases, student loans, and utilities. FBCS received Plaintiff's and Class Members' PII from its clients, which is used to collect debts on behalf of its clients. One of FBCS's clients is Kohl's.

3. Kohl's is one of the largest department store chains in the United States with more than 1,100 locations, operating in every U.S. state except Hawaii.[1] In addition to operating retail stores, Kohl's also sells credit cards.[2] On information and belief, Kohl's used debt collection company Financial Business and Consumer Solutions, Inc. ("FBCS") in connection with its credit card services.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about April 26, 2024, FBCS announced that certain systems in its network had been subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access ("Data Breach"). In a filing with the Office of the Maine Attorney General, FBCS confirms that the PII of 4,253,394 individuals was exposed by the Data Breach.[3]

6. On or about August 15, 2024, Kohl's began sending out notice letters to its customers, stating that Kohl's debt collection agency, FBCS, had experienced a data breach, which it discovered on February 26, 2024.

7. Defendant failed to adequately protect Plaintiff's and Class Members' PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its customers' sensitive data. Hackers targeted and obtained Plaintiff's and Class

[1] https://www.sec.gov/Archives/edgar/data/885639/000089271218000245/ksss-3.htm
[2] https://www.kohls.com/sale-event/my-kohls-charge.jsp
[3] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7e6ff931-a035-480f-a977-e11a8af7f768.html

Members' PII because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Defendant also failed to adequately protect Plaintiff's and Class Members' PII by virtue of its failure to vet its vendors—here, FBCS—and ensure they were submitting PII to an entity with adequate data security practices and that its vendors were deleting or archiving inactive PII data and files.

9. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) adequately vet its vendor for data security practices; (ii) warn Plaintiff and Class Members of FBCS's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal law.

10. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to ensure that FBCS had adequate and reasonable safeguards and measures in place to protect the PII of Plaintiff and Class Members after that information was transferred and entrusted to FBCS in order to enable FBCS to collect the debt owed by Plaintiff and Class Members to Kohl's. More specifically, Defendant failed to ensure that FBCS had taken and implemented available steps to prevent an unauthorized disclosure of data, and failed to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption, storage, and destruction of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

11. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe in any further transfers of their sensitive data to third parties and they should be entitled to injunctive and other equitable relief.

12. Plaintiff and Class Members have suffered injury as a result of Kohl's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

13. Plaintiff and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

II. PARTIES

14. Plaintiff Michael Martinez is a citizen and resident of Arizona.

15. Kohl's is a Wisconsin corporation with its headquarters and principal place of business located in Menomonee Falls, Wisconsin.

III. JURISDICTION AND VENUE

16. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class

members who are diverse from Defendant, and (4) there are more than 100 Class members.

17. The Court has personal jurisdiction over Kohl's because it purposely availed itself of the laws of the state of Pennsylvania by operating multiple retail locations there and offering its credit card services to residents of Pennsylvania.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to this action occurred in this District, and Defendant is subject to the Court's personal jurisdiction with respect to this action.

IV. FACTUAL ALLEGATIONS

A. *Defendant's Business*

19. As previously alleged, Kohl's is one of the largest department store chains in the United States with more than 1,100 locations, operating in almost every U.S. state. In addition to operating retail stores, Kohl's also sells credit cards.[4]

20. Kohl's is one of FBCS's clients. Plaintiff provided his PII to Kohl's in connection with a credit card, and Kohl's, in turn, provided the PII to FBCS to collect a debt.

21. On information and belief, FBCS accumulates highly private PII of its clients' customers, which is used to collect debts on behalf of its clients, such as Kohl's.

22. Plaintiff provided his PII to Kohl's as a condition for opening and maintaining an account with Kohl's, and Kohl's, in turn, provided the PII to FBCS to collect an alleged debt.

23. The information held by FBCS in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members, as provided by Kohl's.

24. Upon information and belief, FBCS made promises and representations to its clients, including Kohl's, that the PII collected from them, including that of Plaintiff and Class

[4] *See* https://www.kohls.com/feature/privacy-policy.jsp#scope.

Members, would be kept safe and confidential, that the privacy of that information would be maintained, and that FBCS would delete any sensitive information after it was no longer required to maintain it.

25. Likewise, Kohl's, for its part, made implicit promises and representations to its customers, including Plaintiff and Class Members, that the PII collected from them would be kept safe and confidential, that the privacy of that information would be maintained in accordance with industry standards and the law, and that it would delete any sensitive information after it was no longer required to maintain it.

26. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

27. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant had a legal duty to keep its customers' PII safe and confidential.

28. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

B. *The Data Breach*

31. According to FBCS's filing with the Office of the Maine Attorney General, FBCS discovered the vulnerability on February 26, 2024, but did not notify consumers of the Data Breach until April 26, 2024.[5]

32. The Notice of Data Event, posted on the Office of the Maine Attorney General's website, provides:

> On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact computer systems outside of FBCS's network. We immediately took steps to secure the impacted environment and launched an investigation with the assistance of third-party computer forensics specialists to determine the full nature and scope of the incident. The investigation determined that the environment was subject to unauthorized access between February 14 and February 26, 2024, and the unauthorized actor had the ability to view or acquire certain information on the FBCS network during the period of access. Therefore, FBCS undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected and to whom it related. We are notifying you because certain information related to you may have been accessed or exfiltrated during the incident. This notification was not delayed as a result of a law enforcement investigation.[6]

33. FBCS's filing with the Office of the Maine Attorney General also specifies that FBCS's customers' names or other personal identifiers in combination with driver's license numbers or non-driver identification card numbers were acquired by an external system breach (hacking).[7]

34. In August 2024, Kohl's began sending out its own notice of breach letters ("Kohl's

[5] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7e6ff931-a035-480f-a977-e11a8af7f768.html.
[6] *Id., See* Notice of Data Event.
[7] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/7e6ff931-a035-480f-a977-e11a8af7f768.html.

Notice"). The Kohl's Notice states:

> **What Happened?** On February 26, 2024, FBCS discovered unauthorized access to certain systems in its network. This incident did not impact Kohl's own network or systems. Based on FBCS's investigation, an unauthorized actor accessed FBCS's environment between February 14 and February 26, 2024. FBCS also stated as of July 10, 2024, it determined that the information of individuals, including you, may have been acquired by the unauthorized actor during the incident.
>
> **What Information Was Involved?** The information for affected individuals varied and may have included name, Social Security number, date of birth, and account information (mailing address, email address, partial account numbers).[8]

35. Omitted from both the Notice of Data Breach and the Kohl's Notice are the details of the root cause of the Data Breach, the vulnerabilities exploited, and the specific remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

36. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

37. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII. Nor did Defendant take the precautions and measures needed to adequately vet its vendor, FBCS, to ensure FBCS's data security protocols were sufficient to protect the PII of Kohl's customers, which Kohl's turned over to FBCS.

[8] *See* Ex. A, Notice of Data Breach.

38. The attacker accessed and acquired files containing unencrypted PII of Plaintiff and Class Members. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

39. Plaintiff further believes his PII, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

C. *Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.*

40. Kohl's derives a substantial economic benefit from providing products and services to its customers, and as a part of providing those products and services, Defendant retains and stores the PII of customers, including that of Plaintiff and Class Members.

41. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting the PII from disclosure, and making sure the PII was safe in the hands of any vendors to which Kohl's provided that highly sensitive information.

42. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

43. Plaintiff and Class Members relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, to provide the information to trusted and secure vendors and other third parties, and to make only authorized disclosures of this information.

44. Defendant could have prevented this Data Breach by properly securing the PII of Plaintiff and Class Members and ensuring that their vendors did the same.

45. Upon information and belief, Defendant made promises to consumers to maintain and protect PII, demonstrating an understanding of the importance of securing PII.

46. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. *Defendant Knew or Should Have Known of the Risk Because Institutions in Possession of PII Are Particularly Susceptible to Cyberattacks.*

47. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store PII, like Defendant, preceding the date of the Data Breach.

48. Data thieves regularly target companies that receive and maintain PII due to the highly sensitive nature of that information in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[9]

50. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known the PII it collected and maintained would be targeted by cybercriminals.

51. As custodians of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result

[9] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (https://notified.idtheftcenter.org/s/), at 6.

of a breach.

52. Defendant was, or should have been, fully aware of the unique type and the significant volume of data it provided to FBCS, and, thus, the significant number of individuals who would be harmed by the exposure of that data.

53. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

54. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members, and Defendant's failure to adequately vet their vendor, FBCS.

55. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

E. ***Value of Personally Identifiable Information***

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[11]

[10] 17 C.F.R. § 248.201 (2016).
[11] *Id.*

57. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[12]

58. For example, PII can be sold at a price ranging from $40 to $200.[13] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[14]

59. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach—names and Social Security numbers—is impossible to "close" and difficult, if not impossible, to change.

60. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[15]

61. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing, or even give false information to police.

62. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also

---

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[14] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[15] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study 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.[16]

F. *Defendant Failed to Comply with FTC Guidelines.*

63. The FTC has promulgated numerous guides for businesses which 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.

64. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

65. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for

[16] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of their data security practices, and those of their vendors. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

68. Defendant was at all times fully aware of its obligation to protect the PII of customers, yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

G. *Defendant Failed to Comply with Industry Standards.*

69. As noted above, experts studying cybersecurity routinely identify institutions like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

70. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Kohl's, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees

can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all these industry best practices.

71. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

72. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

H. *Defendant Breached Its Duties to Safeguard Plaintiff's and Class Members' PII.*

74. In addition to their obligations under federal laws, Defendant owed duties to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed duties to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately

protected the PII of Class Members.

75. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of PII in a timely manner.

76. Defendant owed a duty to Plaintiff and Class Members to properly vet all third parties to whom they provided the PII of their employees and/or customers, including FBCS.

77. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

78. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

79. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of their data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to adequately vet their vendors to ensure they maintained sufficient data security practices;

b. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

c. Failing to adequately protect customers' PII;

d. Failing to properly monitor their own data security systems for existing intrusions;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching their duties and obligations to protect Plaintiff's and Class

Members' PII.

80. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access their computer network and systems which contained unsecured and unencrypted PII.

81. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

I. ***Common Injuries & Damages***

82. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of FBCS and Kohl's, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

J. ***The Data Breach Increases Victims' Risk of Identity Theft.***

83. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

84. The unencrypted PII of Class Members will end up for sale on the dark web because

that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

85. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

86. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

87. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

88. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[17]

[17] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and

89. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

90. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, driver's license numbers, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

K. ***Loss of Time to Mitigate Risk of Identity Theft and Fraud***

91. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual

more. As a rule of thumb, the more information you have on a victim, the more money can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

to greater financial harm—yet, the resource and asset of time has been lost.

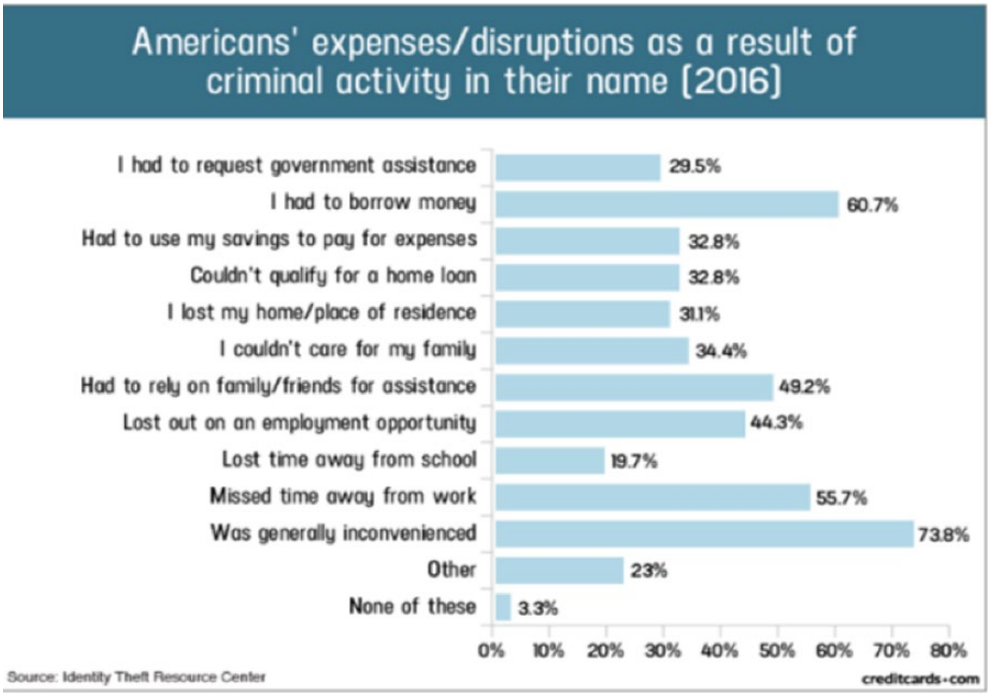
92. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

93. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[18]

94. These efforts are also consistent with the steps the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering 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.[19]

95. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[20]

[18] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[19] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps.
[20] Jason Steele, "Credit Card and ID Theft Statistics," Oct. 24, 2017, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.



L. ***Diminution of Value of PII***

96. PII is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates beyond a doubt that PII has considerable market value.

97. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[21]

98. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[22,]

99. Consumers who agree to provide their web browsing history to the Nielsen

[21] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[22] https://datacoup.com/.

Corporation can receive up to $50.00 a year.[23]

100. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[24]

101. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

M. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary*

102. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchased by criminals intending to utilize the PII for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

103. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's

[23] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.
[24] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

authentic tax return is rejected.

104. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

105. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

N. ***Plaintiff's Experience***

106. Plaintiff is a former customer of Kohl's. Plaintiff gave Kohl's his PII as a condition to opening and maintaining credit card through Kohl's credit card program. In turn, on information and belief, Kohl's gave FBCS Plaintiff's PII in connection with FBCS's debt collection services.

107. Plaintiff provided his PII to Kohl's and trusted the company would use reasonable measures to protect it according to state and federal law. Defendant obtained and continue to maintain Plaintiff's PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

108. Plaintiff received a Notice Letter from Kohl's dated August 15, 2024, informing him that his PII was included in the Data Breach. In it, Kohl's confirmed that Plaintiff's name, address, Social Security number, date of birth, email address, and account information were impacted in the Data Breach.

109. At the time of the Data Breach, Defendant retained Plaintiff's and Class Members' PII in its systems, had provided FBCS Plaintiff's PII, and FBCS retained Plaintiff's PII in its systems.

110. Plaintiff's and Class Members' PII was compromised in the Data Breach and stolen by cybercriminals.

111. Plaintiff has been injured by the compromise of his PII.

112. Plaintiff takes reasonable measures to protect his PII. He has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

113. Plaintiff stores any documents containing his PII in a safe and secure location and diligently chooses unique usernames and passwords for his online accounts.

114. Had Plaintiff known that Kohl's provided sensitive customer PII to vendors, including FBCS, for its business purposes without vetting the vendors' data security adequacy, Plaintiff would not have agreed to be a customer of Kohl's or open a credit card account with Kohl's.

115. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach to protect himself from identity theft and fraud. He has monitored and continues to monitor his accounts, credit reports and credit scores, and has sustained emotional distress. This is time that was lost and unproductive and took away from other activities and duties.

116. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam text messages and phone calls. This misuse of PII is traceable to the Data Breach because cybercriminals routinely obtain information (e.g., phone numbers and email addresses) which can be found online and then target data breach victims with scam calls and messages (i.e., phishing) to elicit more sensitive information—which cybercriminals then combine with the PII exposed in a data breach to commit substantial identity theft and fraud. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach. Because of the Data

Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

117. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that was entrusted to Defendant, which was compromised in and as a result of the Data Breach.

118. Plaintiff suffered lost time, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

119. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, being placed in the hands of criminals that will continue for his lifetime.

120. Defendant obtained and continue to maintain, and continue to allow FBCS to maintain, Plaintiff's PII, and thus have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff's PII was compromised and disclosed as a result of the Data Breach.

121. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

122. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks certification of the following nationwide class:

> All individuals residing in the United States whose PII was compromised in the Data Breach, including all individuals who received notice of the Data Breach ("Class").

123. Excluded from the Class are Defendant and their parents or subsidiaries, any entities in which it has a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

124. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as to add subclasses, before the Court determines whether certification is appropriate.

125. The proposed Class meets the criteria for certification under Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3).

126. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiff believes the proposed Class includes at least 1,955,385 individuals whose Personal Information was compromised in the Data Breach. The precise number of Class Members is unknown to Plaintiff but may be ascertained from Defendant's records.

127. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII

compromised in the Data Breach;

e. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Defendant's data security systems, prior to and during the Data Breach, were consistent with industry standards;

g. Whether Defendant owed duties to Class Members to safeguard their PII;

h. Whether Defendant breached their duties to Class Members to safeguard their PII;

i. Whether hackers obtained Class Members' PII via the Data Breach;

j. Whether Defendant had legal duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendant breached its duties to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

l. Whether Defendant knew or should have known its data security systems and monitoring processes were deficient;

m. What damages Plaintiff and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached express and/or implied contracts with Plaintiff and Class Members;

p. Whether Defendant was unjustly enriched;

q. Whether Plaintiff and Class Members are entitled to damages;

r. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

128. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

129. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

130. Predominance. Defendant has engaged in common courses of conduct toward Plaintiff and Class Members. For example, all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

131. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore 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, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

132. Class certification is also appropriate under Federal Rule of Civil Procedure 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

133. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CLAIMS FOR RELIEF

COUNT I
Negligence and Negligence Per Se
(On Behalf of Plaintiff and the Class Against Kohl's)

134. Plaintiff incorporates and realleges all preceding paragraphs as if fully set forth herein.

135. Plaintiff and Class Members provided their PII to Kohl's as a condition of receiving services.

136. Kohl's had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

137. By assuming the responsibility to collect and store this data, Kohl's had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

138. Kohl's had a duty to employ reasonable security measures under Section 5 of the FTCA, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

139. Kohl's owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

140. Moreover, Kohl's had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

141. Kohl's had and continues to have duties to adequately disclose that the PII of Plaintiff and Class Members within Kohl's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

142. Kohl's breached its duties, pursuant to the FTCA and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Kohl's include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII, including in choosing its vendors

b. Failing to hold vendors with whom it shared sensitive Private Information to adequate standards of data protection;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

143. Kohl's violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Kohl's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

144. Plaintiff and Class Members were within the class of persons the FTCA was intended to protect and the type of harm that resulted from the Data Breach was the type of harm this statute was intended to guard against.

145. Kohl's violation of Section 5 of the FTCA constitutes negligence per se.

146. 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 Plaintiff and Class Members.

147. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class

Members was reasonably foreseeable, particularly in light of Kohl's inadequate security practices.

148. It was foreseeable that Kohl's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches at large corporations that collect and store PII.

149. Kohl's had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

150. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Kohl's knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class Members, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its systems.

151. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

152. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Kohl's possession.

153. Kohl's was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

154. Kohl's duties extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

155. Kohl's has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

156. But for Kohl's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

157. There is a close causal connection between Kohl's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and Class Members was lost and accessed as the proximate result of Kohl's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

158. As a direct and proximate result of Kohl's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kohl's possession and is subject to further unauthorized disclosures so long as Kohl's fails to undertake appropriate and adequate measures to protect the PII.

159. As a direct and proximate result of Kohl's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

160. Additionally, as a direct and proximate result of Kohl's negligence, Plaintiff and

Class Members have suffered and will suffer the continued risks of exposure of their PII, which remain in Kohl's possession and is subject to further unauthorized disclosures so long as Kohl's fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

161. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

162. Kohl's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

163. Plaintiff and Class Members are also entitled to injunctive relief requiring Kohl's to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class Against Kohl's)

164. Plaintiff incorporates and realleges all preceding paragraphs as if fully set forth herein.

165. Kohl's offered to provide products and services to its customers, including Plaintiff and Class Members, in exchange for payment and/or interest.

166. Kohl's also required Plaintiff and Class Members to provide it with their PII in order to receive its products and/or services.

167. In turn, Kohl's impliedly promised to protect Plaintiff's and Class Members' PII through adequate data security measures.

168. Plaintiff and Class Members accepted Kohl's offer by providing their valuable PII to Kohl's in exchange for Plaintiff and Class Members receiving Kohl's products and services,

and then by paying for and receiving the same.

169. Plaintiff and Class Members would not have done the foregoing but for the above-described agreement with the company.

170. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Kohl's in exchange for, amongst other things, the protection of such information.

171. Plaintiff and Class Members fully performed their obligations under the implied contracts with Kohl's.

172. However, Kohl's breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

173. In sum, Plaintiff and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Kohl's.

174. As a reasonably foreseeable result of the Data Breach, Plaintiff and Class Members were harmed by Kohl's failure to use reasonable data security measures to store their PII, including but not limited to, the actual harm through the loss of their PII to cybercriminals.

175. Accordingly, Plaintiff and Class Members are entitled to damages in an amount to be determined at trial, along with their costs and attorneys' fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class Against Kohl's)

176. Plaintiff incorporates and realleges all preceding paragraphs as if fully set forth herein.

177. This count is brought in the alternative to Plaintiff's breach of express and/or

implied contract claims.

178. Upon information and belief, Kohl's funds its data security measures entirely from its general revenue, including from payments made by or on behalf of its clients for services.

179. As such, a portion of the value and monies derived from payments made by its clients for services is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Kohl's.

180. Plaintiff and Class Members conferred a monetary benefit on Kohl's in providing it with their valuable PII.

181. Kohl's knew that Plaintiff and Class Members conferred a benefit which Kohl's accepted. Kohl's profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

182. In particular, Kohl's enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Kohl's instead calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Kohl's decision to prioritize its own profit over the requisite security.

183. Kohl's failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

184. Under the principles of equity and good conscience, Kohl's should not be permitted to retain the benefits that Plaintiff and Class Members conferred upon it.

185. Plaintiff and Class Members have no adequate remedy at law.

186. As a direct and proximate result of Kohl's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) an increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Kohl's possession and is subject to further unauthorized disclosures so long as Kohl's fails to undertake appropriate and adequate measures to protect the PII.

187. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Kohl's and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Kohl's from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

PRAYER FOR RELIEF

WHEREFORE**,** Plaintiff, on behalf of himself and Class Members, requests judgment against Defendant and that the Court enter an Order:

A. certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class, pursuant to Federal Rule of Civil Procedure 23;

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

C. Granting injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to:

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

ii. 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;

iii. requiring Defendant to create a vendor vetting process that thoroughly analyses their vendors' data security practices to ensure they are in compliance with state and federal law and industry standards;

iv. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff 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 Plaintiff and Class Members;

v. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. 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;

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

ix. 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;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. 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 Plaintiff and Class Members;

xii. 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;

xiii. requiring Defendant to implement a system of tests to assess their 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;

xiv. 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;

xv. 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;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. 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.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: October 9, 2024

Respectfully submitted,

By: */s/ Charles E. Schaffer*

Andrew W. Ferich (PA I.D. 313696)
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel.: 310)-474-9111
Fax: 310-474-8585
aferich@ahdootwolfson.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel: 954-525-4100
ostrow@kolawyers.com

Charles E. Schaffer (PA I.D. 76259)
LEVIN SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: 215-592-1500
cschaffer@lfsblaw.com

John A. Yanchunis*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 North Franklin Street 7th Floor
Tampa, FL 33602
Tel: 813-223-5505
JYanchunis@forthepeople.com

Counsel for Plaintiff & the Putative Class

**pro hac vice* pending or to be filed

ClassAction.org
