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

| | |
|---|---|
| ROBERT FARBER, on behalf of himself and all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>H&K PERFORATING, LLC,<br><br>Defendant. | Case No. 1:22-cv-6519<br><br>CLASS ACTION<br><br>JURY TRIAL DEMANDED |

# CLASS ACTION COMPLAINT

Plaintiff, Robert Farber ("Mr. Farber" or "Plaintiff"), brings this action on behalf of himself and all others similarly situated against Defendant, H&K Perforating LLC ("H&K" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

## INTRODUCTION

1. Between March 2 and March 5, 2022, H&K, a manufacturer of perforated metal, lost control over its current and former employees' highly sensitive personal information in a data breach ("Data Breach"), and then failed to start notifying the victims about the breach for more than six months.

2. On information and belief, H&K identified unusual activity on its network on March 5, 2022, and later concluded the Data Breach occurred several days prior to its discovery. However, upon information and belief, even now, H&K has *not* definitively concluded the unauthorized intrusion has been blocked from its system.

3. Upon information and belief, the Data Breach resulted from a ransomware attack on H&K's systems. H&K's investigation revealed that cybercriminals gained unauthorized access

to current and former employees' personally identifiable information ("PII") and personal health information ("PHI") stored on Defendant's network.

4. On information and belief, cybercriminals bypassed Defendant's inadequate security systems to access employees' PII and PHI in its computer systems.

5. On information and belief, the stolen PII and PHI included, at least, employees' names, addresses, Social Security numbers, driver license numbers, financial accounting information, medical/health information, username and email and password and digital/electronic signatures.

6. On or around August 19, 2022—over five months after H&K first discovered the Data Breach—H&K finally began notifying victims about the breach (the "Breach Notice").[1]

7. Defendant's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its employees how many people were impacted, how the breach happened, or why it took the Defendant over five months to begin notifying victims that hackers had gained access to highly sensitive employee information.

8. After discovering the Data Breach in March 2022, H&K's investigation inexplicably dragged on for months and breach victims were not notified that their PII and PHI was at risk until at least August 19, 2022.

9. Following the Data Breach, H&K did not notify its employees in the "most expedient time possible and without unreasonable delay," as required by Illinois law. It is unclear when employees began receiving notices of the Data Breach, if any.

10. In that time, employees were unable to proactively mitigate the Data Breach's impact on them or protect their identities from theft.

[1] The Breach Notice is available on H&K's website https://hkperf.com/ (last visited November 17, 2022).

11. Defendant's failure to timely detect and report the Data Breach made its current and former employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII and PHI.

12. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII and PHI misuse.

13. In failing to adequately protect employees' information, adequately notify them about the breach, and obfuscating the nature of the breach, Defendant violated applicable law and harmed thousands of its current and former employees.

14. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII and PHI. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

15. Mr. Farber is a former H&K employee and Data Breach victim, receiving H&K's Breach Notice in August 2022.

16. By obtaining, collecting, using, and deriving a benefit from the PII and PHI 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. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

17. Accordingly, Plaintiff, on his own behalf and on behalf of a Class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together

with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

18. As a direct and proximate result of Defendant's data security failures and the Data Breach, the PII and PHI of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party, and Plaintiff and Class Members have suffered actual, present, and concrete injuries. These injuries include: (i) the current and imminent risk of fraud and identity theft (ii) lost or diminished value of PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (v) the continued and certainly increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain 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 and PHI; (vi) the invasion of privacy; (vii) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and the Class Members' PII and PHI; and (viii) emotional distress, fear, anxiety, nuisance and annoyance related to the theft and compromise of their PII and PHI.

19. 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 remains at risk due to inadequate data security.

20. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to damages, injunctive and other equitable relief to remedy the harm that resulted from Defendant's inadequate security practices.

## PARTIES

21. Plaintiff, Robert Farber is a natural person and Pennsylvania citizen, residing in Carbondale, Pennsylvania, where he intends to remain.

22. Defendant H&K is an Illinois corporation with its principal place of business located at 5420 W. Roosevelt Road, Suite 314, Chicago, IL 60644.

## JURISDICTION & VENUE

23. This Court has subject-matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

24. This Court has general personal jurisdiction over H&K because it is incorporated in Illinois and its principal place of business is located in Illinois.

25. Venue is proper in this Court because H&K is headquartered in this District.

## BACKGROUND FACTS

### H&K

26. H&K describes itself as a manufacturing company of value-added perforated metal that has been in business for over 135 years.[2] H&K has manufacturing facilities in Illinois, Pennsylvania and Tennessee.

27. On information and belief, H&K accumulates and stores indefinitely the highly sensitive PII and PHI of its employees.

28. On information and belief, H&K requires that its employees disclose their PII and PHI as part of their employment with H&K, including at least their names, dates of birth, Social Security numbers, addresses and driver's license numbers, financial accounting information, medical/health information, username and email and password and digital/electronic signatures.

29. Despite recognizing its duty to do so, on information and belief, H&K has not implemented reasonable cybersecurity safeguards or policies to protect employee PII and PHI or trained its IT or data security employees to prevent, detect, and stop breaches of H&K's systems. As a result, H&K leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to employee PII and PHI

### H&K Fails to Safeguard Employees' PII and PHI

30. Plaintiff and the proposed Class are current and former H&K employees.

31. H&K requires its employees to provide it with their PII and PHI as a condition of employment at H&K.

32. H&K collects and maintains employee PII and PHI in its computer systems.

[2] https://hkperf.com/ (last visited November 17, 2022)

33. In collecting and maintaining the PII and PHI, H&K implicitly agrees it will safeguard the data using reasonable means according to its internal policies, as well as state and federal law.

34. Despite its duties to safeguard employee PII and PHI, beginning on or around March 2, 2022, cybercriminals bypassed H&K's inadequate security systems undetected and accessed employee information.

35. On or around March 5, 2022, H&K identified unusual network activity and eventually determined that cybercriminals had accessed employee PII and PHI.

36. Defendant's investigation revealed that its network had been hacked by cybercriminals and that Defendant's inadequate cyber and data security systems and measures allowed those responsible for the cyberattack to obtain files containing a treasure trove of thousands of H&K employees' personal, private, and sensitive information.

37. Employees place value in data privacy and security. These are important considerations when deciding where to work. Plaintiff would not have accepted the Defendant's employment offer, nor provided his PII or PHI, to H&K had he known that H&K does not take all necessary precautions to secure the personal and financial data given to it by its employees.

38. Despite its duties and alleged commitments to safeguard PII and PHI, H&K does not follow industry standard practices in securing employees' PII and PHI, as evidenced by the Data Breach and stolen employee PII and PHI.

39. In response to the Data Breach, H&K contends that it "with the assistance of third-party forensic specialists" it "deployed countermeasures to contain the event.". H&K's Breach Notice states that it "undertook a comprehensive review of the data to understand the specific

information potentially impacted and to whom it related." *Id.* However, for Data Breach victims, H&K's inability to guarantee data security following the attack, is concerning.

40. Through its Breach Notice, H&K also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft by reviewing account statements and credit reports for unusual activity and report any suspicious activity immediately to their financial institution."

41. H&K has not offered complimentary credit monitoring services to victims, even though victims face a lifetime of harm following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers and birth dates.

42. The risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII and PHI is unacceptably high. The fraudulent activity resulting from the Data Breach may not come to light for years.

43. Cybercriminals need not harvest a person's Social Security number to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

44. On information and belief, H&K failed to adequately train its IT and data security employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over employee PII and PHI. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing PII and PHI Further, the Breach Notice makes clear that H&K cannot, or will not, determine the full scope of the Data Breach.

45. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

46. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it….

- Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….

47. To prevent and detect cyber-attacks attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> Secure internet-facing assets
>
> -Apply latest security updates
> -Use threat and vulnerability management
> -Perform regular audit; remove privileged credentials;
>
> Thoroughly investigate and remediate alerts
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> Include IT Pros in security discussions
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> Build credential hygiene
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> Apply principle of least-privilege
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events;
>
> Harden infrastructure
>
> - Use Windows Defender Firewall
> - Enable tamper protection
> - Enable cloud-delivered protection

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[3]

48. Given that Defendant was storing the PII and PHI of Plaintiff and Class Members, Defendant could and should have implemented all of the above standard measures to prevent and detect cyber-attacks.

49. The occurrence of the Data Breach and Defendant's failure to timely detect it indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyber-attacks, resulting in the Data Breach and the exposure of the PII and PHI of thousands of H&K's current and former employees, including Plaintiff and Class Members.

**Plaintiff's Experience**

50. Plaintiff Farber is a former H&K employee, having worked for the company between January and June 2021.

51. As a condition of his employment, H&K required Plaintiff to provide it with his PII and PHI.

52. Plaintiff provided his PII and PHI to H&K and trusted the company would use reasonable measures to protect it according to H&K's internal policies, as well as state and federal law.

53. To date, Defendant has done nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach.

[3] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited November 17, 2022).

54. Plaintiff typically takes measures to protect his PII and PHI and is very careful about sharing his PII and PHI. Plaintiff has never knowingly transmitted unencrypted PII or PHI over the internet or other unsecured source.

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

56. As a result of the Data Breach, Plaintiff experienced fraudulent charges made on his debit card, including a charge for $1,000 in the spring of 2022. It took Plaintiff's bank 30-days to reimburse Plaintiff for the fraudulently debited amount, causing him loss of those funds in the interim.

57. The Data Breach and resulting identity theft Plaintiff experienced also prevented Plaintiff from timely filing his 2021 tax returns.

58. As a result of the Data Breach, Plaintiff also 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. In response to the Data Breach, Plaintiff has spent significant time monitoring his accounts and credit score and has sustained emotional distress in addition to his lost time. This is time that was lost and unproductive and took away from other activities and duties.

59. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII and PHI—a form of intangible property that he entrusted to Defendant for the purpose of obtaining employment with Defendant, which was compromised in and as a result of the Data Breach.

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

61. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI especially his Social Security Number, being placed in the hands of criminals.

62. Defendant obtained and continues to maintain Plaintiff's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure. Plaintiff's PII and PHI was compromised and disclosed as a result of the Data Breach.

63. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII and PHI was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

**Plaintiff and the Proposed Class Face Significant Risk of Identity Theft**

64. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII and PHI hat can be directly traced to Defendant.

65. The ramifications of H&K's failure to keep Plaintiff and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, without permission, to commit fraud or other crimes.

66. The types of personal data compromised and potentially stolen in the H&K Data Breach is highly valuable to identity thieves. The employees' stolen PII can be used to gain access to a variety of existing accounts and websites to drain assets, bank accounts or open phony credit cards.

67. As a result of H&K's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered, or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of H&K and is subject to further breaches so long as H&K fails to undertake the appropriate measures to protect the PII and PHI in their possession.

68. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[4]

[4] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited November 17, 2022).

69. The value of Plaintiff's and the proposed Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

70. It can take victims years to stop identity or PII theft, giving criminals time to sell that information for cash.

71. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

72. Cybercriminals can cross-reference multiple sources of PII and PHI 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. These dossiers are known as "Fullz" packages.[5]

73. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's 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 may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can 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. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

[5] *Id.*

74. Additionally, Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[6]

75. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

76. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[7]

77. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive

---

[6] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited November 17, 2022).

[7] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited November 17, 2022).

and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

78. H&K's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and thousands of members of the proposed class to unscrupulous operators, con artists and criminals.

79. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

80. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII and PHI.

81. 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 and PHI of Plaintiff and Class Members.

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

**H&K Failed to Adhere to FTC Guidelines.**

83. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

84. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

85. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

86. The FTC recommends that companies not maintain information 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

87. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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 Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

88. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

**CLASS ACTION ALLEGATIONS**

89. Plaintiff brings this action pursuant to FRCP 23(b)(2) and (b)(3) on behalf of himself and all members of the proposed class (the "Class") tentatively defined as:

> All persons whose PII and PHI was compromised in the Data Breach disclosed by H&K in August 2022, including all those who were sent a notice of the Data Breach.

90. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

91. The Class defined above is identifiable through H&K's business records.

92. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

93. This action satisfies the numerosity, commonality, typicality, and adequacy requirements of Fed. R. Civ. P. 23.

**Numerosity**

94. The exact number of Class members is unknown but is estimated to be up to thousands of former and current H&K employees at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, employee breach of contract, unlawful trade practices, and class action controversies.

95. Plaintiff is a member of the Class.

**Commonality, Predominance, and Superiority**

96. There are questions of law and fact common to Plaintiff and to the proposed Class, including but not limited to the following:

a. Whether H&K had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII and PHI;

b. Whether H&K failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether H&K was negligent in maintaining, protecting, and securing PII and PHI;

d. Whether H&K breached contract promises to safeguard Plaintiff's and the Class's PII and PHI;

e. Whether H&K took reasonable measures to determine the extent of the Data Breach after discovering it;

f. Whether H&K's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff and the Class injuries;

h. What the proper damages measure is;

i. Whether H&K violated the statutes alleged in this Complaint; and

j. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

97. Common questions of law and fact predominate over questions affecting only individual class members, and a class action is the superior method for fair and efficient adjudication of the controversy.

98. Plaintiff's claims are typical of the claims of Class members.

**Adequacy**

99. Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class, he will fairly and adequately protect the interests of the Class, and he is represented by counsel skilled and experienced in class actions.

**FIRST CLAIM FOR RELIEF**
**Negligence**
**(On Behalf of Plaintiff and the Class)**

100. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

101. Plaintiff and the Class entrusted Defendant with their PII and PHI.

102. Plaintiff and the Class entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

103. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiff and the Class could and would suffer if the PII and PHI were wrongfully disclosed.

104. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII and PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

105. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII and PHI of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

106. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations.

107. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and the Class.

108. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII and PHI, a necessary part of obtaining employment from Defendant.

109. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

110. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

112. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

113. Plaintiff and the Class had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

114. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

115. Defendant had and continue to have a duty to adequately disclose that the PII and PHI of Plaintiff and the Class within Defendant'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 the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

116. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and the Class.

117. Defendant has admitted that the PII and PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

118. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and the Class during the time the PII and PHI was within Defendant's possession or control.

119. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

120. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and the Class in the face of increased risk of theft.

121. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of PII and PHI.

122. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

123. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, PII and PHI PII of Plaintiff and the Class would not have been compromised.

124. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiff and the Class and the harm, or risk of

imminent harm, suffered by Plaintiff and the Class. The PII and PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

125. Additionally, 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 businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

127. Defendant's violation of Section 5 of the FTC Act constitutes negligence per se.

128. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

130. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer injury, including, but not limited to: (i) actual

identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain 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 and PHI of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

131. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class 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.

132. Additionally, as a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain 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 and PHI in its continued possession.

133. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

**SECOND CLAIM FOR RELIEF**
**Breach of Implied Contract**
**(On Behalf of Plaintiff and the Class)**

134. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

135. Defendant offered to employ Plaintiff and members of the Class in exchange for their PII and PHI.

136. Plaintiff and the members of the Class accepted Defendant's offer by providing PII and PHI to Defendant in exchange for employment with Defendant. Plaintiff and the Class then provided labor services to Defendant.

137. In turn, and through internal policies, Defendant implicitly agreed it would not disclose the PII and PHI it collects to unauthorized persons. Defendant also implicitly promised to safeguard employee PII and PHI.

138. Also implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII and PHI.

139. These agreements were not contained in any express contract.

140. Plaintiff and the members of the Class would not have entrusted their PII and PHI to Defendant in the absence of such agreement with Defendant.

141. Defendant materially breached the contracts it had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly

of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII and PHI;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted.

142. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

143. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

144. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

145. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

146. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

147. In these and other ways, Defendant violated its duty of good faith and fair dealing.

148. Plaintiff and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

149. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

**THIRD CLAIM FOR RELIEF**
**Unjust Enrichment**
**(On Behalf of the Plaintiff and the Class)**

150. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

151. This claim is plead in the alternative to the breach of implied contractual duty claim.

152. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of services through employment. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII and PHI, as this was used to facilitate their employment.

153. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

154. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's services and their PII and PHI because Defendant failed to adequately protect their PII and PHI. Plaintiff and the proposed Class would

not have provided their PII and PHI or worked for Defendant at the payrates they did, had they known Defendant would not adequately protect their PII and PHI.

155. Defendant should be compelled to disgorge into a common fund to benefit Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

**FOURTH CLAIM FOR RELIEF**
**Invasion of Privacy**
**(On Behalf of the Plaintiff and the Class)**

156. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

157. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

158. Defendant owed a duty to its employees, including Plaintiff and the Class, to keep this information confidential.

159. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff's and Class Members' PII and PHI is highly offensive to a reasonable person.

160. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant as part of Defendant's employment, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

161. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

162. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

163. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

164. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

165. As a proximate result of Defendant's acts and omissions, the private and sensitive PII and PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

166. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII and PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

167. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII and PHI of Plaintiff and the Class.

168. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

**FIFTH CLAIM FOR RELIEF**
**DECLARATORY JUDGMENT/INJUNTIVE RELIEF**
**(On Behalf of Plaintiff and the Class)**

169. Plaintiff and the members of the Class incorporate the above allegations as if fully set forth herein.

170. 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 granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

171. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII and PHI, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their PII and PHI. Plaintiff and the Class remain at imminent risk that further compromises of their PII and PHI will occur in the future.

172. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect employees' PII and PHI.

173. Defendant still possesses the PII and PHI of Plaintiff and the Class

174. To Plaintiff's knowledge, Defendant has made no changes to its data storage or

security practices relating to the PII and PHI.

175. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

176. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at H&K. The risk of another such breach is real, immediate, and substantial.

177. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at H&K, Plaintiff and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

178. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at H&K, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other employees whose PII and PHI would be further compromised.

179. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes 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;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII and PHI not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

**PRAYER FOR RELIEF**

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining H&K from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PII and PHI;

E. Awarding Plaintiff and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting such other or further relief as may be appropriate under the circumstances.

**JURY DEMAND**

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

Dated: November 21, 2022

Respectfully submitted,

By: */s/ Samuel J. Strauss*

Samuel J. Strauss
sam@turkestrauss.com
Raina C. Borrelli
raina@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

*Attorneys for Plaintiff and the Proposed Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: H&K Perforating Failed to Prevent 2022 Data Breach, Class Action Says

---