IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

TOBY CLARKSON GARDNER and KESTON LEWIS, on behalf of themselves and all others similarly situated, Plaintiff, v. MATCO TOOLS CORPORATION Defendant.	Case No. 5:23-cv-00383 **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

INTRODUCTION

1. This case arises from a data breach. Defendant Matco Tools Corporation ("Matco") is a professional tool distribution franchise for the automotive and other industries. Matco customers have no choice but to trust Matco to keep their data secure.

2. In a story that has become all too familiar, an unauthorized third-party gained access to Matco's network around March 1, 2022 and absconded with personally identifying and financial information (PII). Criminals can now sell the victims' data on the black market for the purpose of stealing their identities. None of this would have occurred if Matco had implemented reasonable data security measures.

3. Plaintiffs Toby Clarkson Gardner and Keston Lewis were victims of the data breach. They bring this action on behalf of themselves and all others similarly situated, seeking damages for the injuries that Defendant's negligence have and will cause, as well as injunctive relief to ensure that the data Defendant continue to store will be protected by reasonable data security practices going forward.

PARTIES

4. Plaintiff Toby Clarkson Gardner is a resident of the State of Wyoming.

5. Plaintiff Keston Lewis is a resident of the State of Georgia.

6. Defendant Matco Tools Corporation is a Delaware corporation with a principal place of business in Stow, Ohio. Matco made the decisions giving rise to the data breach from its Ohio headquarters.

JURISDICTION AND VENUE

7. Matco is subject to this Court's personal jurisdiction because its principal place of business is (and at all relevant times was) located in Stow, Ohio.

8. This Court has subject-matter jurisdiction under 28 U.S.C. § 1332(d)(2) because at least one member of the proposed Class, including both Clarkson Gardner and Lewis, is a citizen of a state different from that of Matco; the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed Class consists of more than 100 class members, and none of the exceptions under the subsection apply to this action.

9. Venue is proper because Matco's principal place of business is located in the Northern District of Ohio. *See* 28 U.S.C. § 1391(b)(1).

FACTUAL ALLEGATIONS

A. Matco allowed Plaintiffs' data to be stolen.

10. According to the data breach notice that Plaintiffs received, an unauthorized third-party gained remote access to Matco's network on March 1, 2022 acquired information from Plaintiff and Class members. A true and correct copy of the Notice Letter is attached as Exhibit 1.

11. Information pertaining to Plaintiffs and Class members was part of the data acquired by an unauthorized external party in the Data Breach.

12. According to the Notice Letter, upon learning of the breach (at an undisclosed date), Matco conducted an investigation. No details are provided regarding this investigation, other than that "[a] cybersecurity firm was engaged to assist."

13. According to the Notice Letter, on December 8, 2022, the investigation revealed the nature of the breach. The specific information that was acquired includes: name, Social Security number, driver's license number, and/or financial account information.

14. Because this data breach targeted financial and personally identifying information, it is reasonable to infer that the hackers will use victims' data for fraudulent purposes, including identity theft.

15. The Notice Letter Plaintiffs received says that that Class members should obtain credit monitoring and identity theft protection services to help them detect possible misuse of PII. *See* Exhibit 1. Class members are therefore at a substantial risk of identity theft.

16. Nothing in the breach letter describes the cause of the breach, who might have been responsible, or any matters taken by Matco to prevent further breaches in the future.

17. As a result of the Data Breach, Plaintiffs and Class members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

B. The data breach was highly foreseeable, yet Matco failed to take reasonable precautions.

18. Given the type of data that Matco collected and stored, it was highly foreseeable that bad actors would attempt to access it without permission.

19. "[H]ackers are likely to be drawn to databases containing information which has a high value on secondary black markets," such as "identifying and financial data." Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55 (2021). Consequently, "relevant and rational firms should engage in greater security investment

and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification." *Id.* at 855.

20. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

21. Because Matco collected and stored identifying and financial information that is very valuable to criminals, it was highly foreseeable that a bad actor would attempt to access that data without permission.

22. Matco frequently collects and stores personally identifying and financial information. Therefore, the burden (if any) of implementing reasonable data security practices is minimal in comparison to the substantial and highly foreseeable risk of harm.

23. On information and belief, Matco failed to adequately train its employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of multi-factor authentication for all users;

b. Locking, encrypting and limiting access to computers and files containing sensitive information;

c. Implementing guidelines for maintaining and communicating sensitive data;

d. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

e. Providing focused cybersecurity awareness training programs for employees.

24. The FTC has noted the need to factor data security into all business decision-making. *Start With Security, A Guide for Business*, FTC (accessed June 9, 2022), https://bit.ly/3mHCGYz. According to the FTC, data security requires: (1) encrypting

information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software. *Id.*

25. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the data breach, further clarify the measures businesses must take to meet their data security obligations.

26. On information and belief, Matco'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 Classes to unscrupulous operators, con artists, and outright criminals.

27. Matco violated its obligation to implement best practices and comply with industry standards concerning computer system security, which allowed class members' data to be accessed and stolen by criminals.

C. Plaintiffs' information was exposed in the data breach, which caused them to suffer concrete injuries.

28. Plaintiff Toby Clarkson Gardner applied to work for Matco beginning in 2015. He did not ultimately work for Matco, but in the course of the employment application process he provided Matco his name, Social Security number, and Drivers' License Number.

29.

30. Clarkson Gardner received a data breach notification informing him that his personally identifying and financial information was accessed in the breach.

31. Plaintiff Keston Lewis has been a customer of Matco since 2013. As part of those purchases, Plaintiff provided his PII to Matco.

32. Lewis received a data breach notification informing him that his personally identifying and financial information was accessed in the breach.

33. Plaintiffs' PII was compromised in the data breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

34. In particular, Plaintiff Clarkson Gardner was the victim of identity theft, as some unidentified individual residing in California attempted to make a purchase using his bank account.

35. As a result of the data breach, Plaintiffs have suffered a loss of time and have spent and continues to spend time on issues related to this Data Breach. In response to the data breach, Plaintiffs have spent time monitoring their accounts and credit score and have sustained

emotional distress in addition to their lost time. This is time that was lost and unproductive and took away from other activities and duties.

36. Plaintiffs also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Matco—which was compromised in and as a result of the data breach.

37. Plaintiffs suffered lost time, annoyance, interference, and inconvenience as a result of the data breach and has anxiety and increased concerns for the loss of their privacy.

38. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, especially their Social Security numbers, being placed in the hands of criminals.

39. In the case of Plaintiff Clarkson Gardner, these concerns are not theoretical, as his identify was in fact compromised and used for improper purposes.

40. In fact, in approximately March 2022, Plaintiff received a telephone call from Points West Community Bank regarding the fraudulent transactions he did not authorize.

41. Matco continue to maintain Plaintiffs' PII and have a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiffs would not have entrusted their PII to Matco had they known that it would fail to maintain adequate data security. Plaintiffs' PII was compromised and disclosed as a result of the Data Breach.

42. As a result of the Data Breach, Plaintiffs anticipate 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, Plaintiffs are at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

43. Because their personally identifying and financial information has been accessed by criminals, Plaintiffs and the Class have suffered concrete and ongoing injuries.

44. Plaintiffs and the Class are at an imminent and substantial risk of identity theft.

45. According to experts, one out of four data breach notification recipients become a victim of identity fraud. *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, THREATPOST.COM (Feb. 21, 2013), https://bit.ly/3zB8Uwv.

46. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PHI can be worth up to $1,000.00 depending on the type of information obtained. *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 15, 2017), https://bit.ly/2Ox2SGY.

47. The value of Plaintiffs' and the proposed Class's PII on the black market is considerable. Stolen PII 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.

48. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

49. One such example of criminals using PII for profit is the development of "Fullz" packages. "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 more. As a rule of thumb, the more information you have on a victim, the more money can be made off 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://bit.ly/3Qj2eJd.

50. Cyber-criminals can cross-reference two sources of PII to marry unregulated or partial data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete "Fullz" dossiers on individuals.

51. The development of "Fullz" packages means that stolen PHI from the data breach can easily be used to link and identify it to Plaintiffs' 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 likely what is already happening to Plaintiffs and members of the proposed Classes, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the data breach.

52. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

53. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

54. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

55. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by theft of their PII. Victims of

new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

56. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Classes will need to be remain vigilant against unauthorized data use for years or even decades to come.

57. Moreover, the breach has diminished the value of Plaintiff and the Classes' personal information.

58. The FTC has recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency." *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FTC (Dec. 7, 2009), https://bit.ly/3xKfzmu.

59. Since it was included in the breach, Plaintiffs and the Classes' information has already been accessed by criminals, which decreases its value in the marketplace.

60. Therefore, the value of Plaintiffs and the Classes' personal information was reduced by the data breach.

61. Section 5 of the FTC Act, 15 U.S.C. § 45, 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.

62. Defendants 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. Defendants' conduct was particularly unreasonable given the nature and amount of

PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

63. None of those injuries would have occurred if Defendant had implemented reasonable data security practices.

CLASS ACTION ALLEGATIONS

64. Pursuant to FED. R. CIV. P. 23(b)(2) and (b)(3), Plaintiffs seek certification of a Class defined as follows:

> All individuals in the United States whose personal information was compromised in connection with the data breach affecting Matco Tools Corporation on or around March 1, 2022.

65. Excluded from the Class and Subclass are: (a) Defendant and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

66. *Ascertainability.* The Class can be readily identified through Matco's records, which is demonstrated by the fact that many class members have already been identified and sent notice letters regarding the data breach.

67. *Numerosity.* On information and belief, Matco sells products to tens or hundreds of thousands of customers. Therefore, the Class is so numerous that individual joinder is impracticable.

68. *Typicality.* Plaintiffs' claims are typical of the Class he seeks to represent. Like all class members, Plaintiffs' personal information was exposed in the data breach as a result of Defendant's failure to implement reasonable data security measures. Thus, Plaintiffs' claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

69. *Adequacy of Class Representative.* Plaintiffs will fairly and adequately protect the interests of the Class. He is aware of his fiduciary duties to absent class members and is determined to faithfully discharge his responsibility. Plaintiffs' interests are aligned with (and not antagonistic to) the interests of the Class.

70. *Adequacy of Counsel.* In addition, Plaintiffs have retained competent counsel with considerable experience in class action and other complex litigation, including data breach cases. Plaintiffs' counsel have done substantial work in identifying and investigating potential claims in this action, have considerable knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Classes.

71. *Commonality and Predominance.* This case presents numerous questions of law and fact with answers common to the Class that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiffs and the Class's PII;

b. Whether Defendant breached the duty to use reasonable care to safeguard the Class's PII;

c. Whether Defendant breached its contractual promises to safeguard Plaintiffs and the Class's PII;

d. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

e. Whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs and the Class's PII from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendants' computer systems to safeguard and protect Plaintiffs and the Class's PII from unauthorized release and disclosure;

g. Whether the data breach was caused by Defendant's inadequate cybersecurity measures, policies, procedures, and protocols;

h. Whether Defendant took reasonable measures to determine the extent of the data breach after it was discovered;

i. Whether Defendant's delay in informing Plaintiffs and the Class of the data breach was reasonable;

j. Whether Defendant is liable for negligence, gross negligence, or recklessness;

k. Whether Defendant's conduct, practices, statements, and representations about the data breach of the PII violated applicable state laws;

l. Whether Plaintiffs and the Class were injured as a proximate cause or result of the data breach;

m. What the proper measure of damages is; and

n. Whether Plaintiffs and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

72. *Superiority and Manageability.* A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

73. *Injunctive or Declaratory Relief.* In addition, Defendant acted or failed to act on grounds that apply generally to the Classes, such that final injunctive or declaratory relief as to any one class member is appropriate as to all class members.

CAUSES OF ACTION

Count 1: Negligence

74. Plaintiffs incorporate by reference all of the above allegations.

75. Plaintiffs and the Class entrusted their PII to financial institutions who turned that information over to Defendant. Knowing this, Defendant owed to Plaintiffs and other the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the

information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

76. Defendant owed a duty of care to Plaintiffs and the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the data breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs and the Class's PII failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

77. Defendant owed these duties to Plaintiffs and the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiffs and the Class's personal and financial information in the conduct of its business, and Defendant retained that information.

78. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

79. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI and PII of Plaintiffs and the Class and the importance of exercising reasonable care in handling it.

80. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiffs and the Classes, which actually and proximately caused the data breach and Plaintiffs and the Classes injury.

81. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and the Class's actual, tangible, injury-in-fact and damages, including, without limitation, theft of their PII by criminals,

improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the data breach.

Count 2: Negligence Per Se

82. Plaintiffs incorporate by reference all of the above allegations.

83. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

84. 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 customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the members of the Class's sensitive PII.

85. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect its employees' 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 Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its employees in the event of a breach, which ultimately came to pass.

86. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because 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 members of the Class.

87. Defendant had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and the Class's PII.

88. Defendant breached its respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

89. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

90. As a direct and proximate result, Plaintiffs suffered actual losses and damages, including, without limitation, theft of his PII by criminals, improper disclosure of his PII, lost value of his PII, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence.

Count 3: Breach of Implied Contract

91. Plaintiffs incorporate by reference all preceding allegations.

92. Plaintiff Clarkson Gardner and members of the Class provided personal information to Defendant as part of seeking employment from Matco

93. As a condition of seeking that employment, Matco required Plaintiff and the Class to provide it with their PII.

94. Plaintiff Clarkson Gardner and Class Member that sought employment from Matco reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

95. This constitutes an implied contract between potential employees and Matco to safeguard its PII.

96. In addition, Plaintiff Lewis and some members of the Class entered into commercial transactions with Matco. In the context of those transactions, Plaintiff Lewis and Class members were required to provide PII to Matco.

97. Plaintiff Lewis and members of the Class that entered into commercial transactions with Matco reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of the PII they provided.

98. Those transactions represent contractual agreements supported by consideration.

99. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

100. Plaintiffs and the members of the Class would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

101. Defendant materially breached the contract(s) it had entered with Plaintiffs 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.

102. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

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

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.

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

104. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

105. 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.

106. 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.

107. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

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

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

Count 4: Unjust Enrichment

(In the Alternative to Count 3)

110. Plaintiffs incorporate paragraphs 1–83 by reference.

111. Plaintiffs and the Class conferred a benefit on Matco in the form of payments associated with the purchases of goods and/or providing employment services or prospective employment services. Matco also benefitted from the receipt of Plaintiffs and the Class's PII, as this was used for Matco's commercial purposes.

112. Matco knew of the benefits conferred on it by Plaintiffs and the Class.

113. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs and the Class's services and their PII because Matco failed to adequately protect their PII. Plaintiffs and the Class would not have provided their PII to Matco if they had known Matco would not adequately protect their PII.

114. Matco should be compelled to disgorge into a common fund for the benefit of Plaintiffs and the Class all unlawful or inequitable proceeds it received due to its misconduct.

PRAYER FOR RELIEF

115. Plaintiffs, individually and on behalf of all others similarly situated, hereby demand:

a. Certification of the proposed Class;

b. Appointment of the undersigned counsel as class counsel;

c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law;

d. Restitution or disgorgement of all ill-gotten gains; and

e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

116. Plaintiffs demand a jury trial on all applicable claims.

Respectfully submitted,

By: /s/ *Michael J. Boyle, Jr.*

MEYER WILSON CO., LPA
Matthew R. Wilson (Bar No. 0072925)
Email: mwilson@meyerwilson.com
Michael J. Boyle, Jr. (Bar No. 0091162)
Email: mboyle@meyerwilson.com
Jared W. Connors (Bar No. 0101451)
Email: jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice* to be filed)
sam@turkestrauss.com
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703

P: (608) 237-1775

Counsel for Plaintiff and the Proposed Class