

**IN THE COURT OF COMMON PLEAS  
LORAIN COUNTY, OHIO**

COLTON MCCLINTOCK, TANNER  
WOLCOTT, and ALICIA WOLCOTT,  
individually and on behalf of all others  
similarly situated,

Plaintiffs,

v.

ELYRIA FOUNDRY HOLDINGS, LLC and  
ELYRIA FOUNDRY COMPANY LLC,

Defendants.

Case No: No. 24-cv-214017

Judge: Honorable Judge Rothgery

COMPLAINT – CLASS ACTION  
DEMAND FOR JURY TRIAL

Plaintiffs Colton McClintock, Tanner Wolcott, and Alicia Wolcott (“Plaintiffs”), individually and on behalf of all others similarly situated, sues Elyria Foundry Holdings, LLC (“Elyria” or “Defendant”), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

**I. INTRODUCTION**

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendants (the “Data Breach”), which held in its possession certain personally identifiable information (“PII” or the “Private Information”) of its current and former employees (and their spouses and dependents), the putative class members (“Class”). This Data Breach occurred between June 24 and June 25, 2024.

2. The Private Information compromised in the Data Breach included certain personal information of Defendants' current and former employees and their spouses and dependants, including Plaintiffs. According to the Notice of Security Incident Elyria mailed to victims, the Private Information includes at least names and Social Security numbers.

3. The Private Information was stolen by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals. In total, Defendants injured at least 2,193 persons—via the exposure of their Private Information—in the Data Breach. Upon information and belief, these 2,193 persons include their current and former employees (and their spouses and dependents).<sup>1</sup>

4. On information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train their employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Private Information. In short, Defendants' failures placed the Class's Private Information in a vulnerable position—rendering them easy targets for cybercriminals.

5. In other words, Defendants had no effective means to prevent, detect, stop, or mitigate breaches of their systems—thereby allowing cybercriminals unrestricted access to their current and former employees' (and their spouses' and dependents') Private Information.

6. Plaintiffs bring this class action lawsuit on behalf of themselves and those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs

---

<sup>1</sup> Elyria Foundry Holdings, LLC, *Data Breach Notifications*, Office of the Maine Atty. Gen. (Sept. 3, 2024), <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b887959e-2c69-498b-9873-e35f2baf9c2d.html> (last visited Dec. 17, 2024).

and other Class Members that their information was subjected to unauthorized access by an unknown third party.

7. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

8. Defendants, through their employees, disregarded the rights of Plaintiffs and Class Members by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Defendants also failed to disclose that they did not have adequately robust computer systems and security practices to safeguard Plaintiffs' and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

9. In addition, Defendants' employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendants' employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct since the Private Information that Defendants collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class

Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

12. Because of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. Plaintiffs are Data Breach victims, having received breach notices. Plaintiff McClintock's Breach Notice is attached as Exhibit A and Plaintiff Tanner Wolcott's Breach Notice is attached as Exhibit B. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

16. Accordingly, Plaintiffs sue Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract, (iii) breach of fiduciary duty, (iv) unjust enrichment, and (v) declaratory judgment.

## **II. PARTIES**

17. Plaintiff, Colton McClintock, is a natural person and citizen of Ohio, residing in Lorain where he intends to remain.

18. Plaintiff, Tanner Wolcott, is a natural person and citizen of Pennsylvania, residing in Greenville where he intends to remain.

19. Plaintiff, Alicia Wolcott, is a natural person and citizen of Pennsylvania, residing in Greenville where she intends to remain.

20. Defendant Elyria Foundry Holdings, LLC, is a Delaware limited liability company that operates foundry businesses in Ohio, with its principal place of business at 120 Filbert Street, Elyria, Ohio 44035.

21. Defendant, Elyria Foundry Company LLC, is a limited liability company formed under the laws of Delaware and with its principal place of business in Elyria, Ohio.

## **III. JURISDICTION AND VENUE**

22. This Court has original jurisdiction over this action pursuant to Article IV, § 4 of the Ohio Constitution and O.R.C. § 2305.01.

23. This Court has personal jurisdiction over Defendants pursuant to O.R.C. § 2307.382 because Elyria conducts business in Ohio and the acts and omissions complained of occurred within this state.

24. Venue is proper in this Court pursuant to Ohio Civ. R. 3(C)(3) because Defendants have their principal place of business in Lorain County and the acts and omissions complained of occurred within this county.

#### IV. FACTUAL ALLEGATIONS

##### *Defendants' Business*

25. Elyria is a metal casting company that operates the Elyria Foundry in Elyria, Ohio and Hodge Foundry in Greenville, Pennsylvania.<sup>2</sup>

26. In the ordinary course of applying for and/or obtaining employment with Elyria, each employee was required to provide (and Plaintiffs did provide) Defendants with sensitive, personal, and private information, such as their:

- address;
- telephone number;
- date of birth;
- Social Security number;
- driver's license number;
- driver's license state.

27. All of Defendants' human resources employees and staff may share employee information with each other for various purposes.

28. In collecting and maintaining the Private Information, Defendants agreed they would safeguard the data in accordance with their internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information.

29. Under state and federal law, businesses like Defendants have duties to protect their current and former employees' (and their spouses' and dependents') Private Information and to notify them about breaches.

30. Defendants recognize these duties, declaring in their "Privacy Policy" that:

---

<sup>2</sup> *Hodge Foundry, supra*, <https://www.elyriafoundry.com/hodge-foundry/> (last visited Dec. 18, 2024).

- a. “This Privacy Policy Statement (the ‘Privacy Statement’) explains how [Defendant] collects, uses, stores, processes, discloses and deletes Personal Data (as defined herein) you provide directly to us[.]”<sup>3</sup>
- b. “We are committed to protecting your privacy.”<sup>4</sup>
- c. “Any information provided is securely stored with our business partners and other organizations and individuals with which we have established a strategic alliance or other contractual relationship.”<sup>5</sup>
- d. “We are committed to ensuring the security of your Personal Data.”<sup>6</sup>
- e. “In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the information we collect[.]”<sup>7</sup>

31. The employee information held by Defendants in its computer system and network included the Private Information of Plaintiffs and Class Members.

### ***The Data Breach***

32. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendants.

33. On June 24, 2024, Defendants were hacked in the Data Breach.<sup>8</sup>

---

<sup>3</sup> *Privacy Policy*, Elyria Foundry (August 2019), <https://www.elyriafoundry.com/elyria-foundry/privacy-policy/> (last visited Dec. 17, 2024).

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> *Id.*

<sup>7</sup> *Id.*

<sup>8</sup> *Notice of Data Privacy Event*, Elyria Foundry (Sept. 3, 2024), <https://www.elyriafoundry.com/media/hhucfcug/elyria-web-notice.pdf> (last visited Dec. 18, 2024).

34. According to Defendants' Notice of Security Incident,

On June 25, 2024, we became aware of suspicious activity in our computer network. We quickly secured our network and hired outside specialists to help us investigate. The investigation found that for a few hours between June 24, 2024, and June 25, 2024, an unknown actor accessed part of our network and may have viewed and/or copied some of our files. In response, we reviewed the affected files to identify whether those files contained any personal information. Our review found that information about current and former employees and their spouses and dependents may have been impacted by this incident.

...

Your name and Social Security number may have been present in the affected files. The investigation did not confirm whether your information was actually viewed or taken, but we cannot rule out this possibility. We have no indication of identity theft or fraud related to this incident.

35. In total, Defendants injured at least 2,193 persons—via the exposure of their Private Information—in the Data Breach. Upon information and belief, these 2,193 persons include their current and former employees (and their spouses and dependents).<sup>9</sup>

36. And yet, Defendants waited until September 3, 2024, before they began notifying the class—a full 71 days after the Data Breach began.<sup>10</sup>

37. Thus, Defendants kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

38. And when Defendants did notify Plaintiffs and the Class of the Data Breach, Defendants acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class:

---

<sup>9</sup> Elyria Foundry Holdings, LLC, *Data Breach Notifications*, Office of the Maine Atty. Gen. (Sept. 3, 2024), <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b887959e-2c69-498b-9873-e35f2baf9c2d.html> (last visited Dec. 18, 2024).

<sup>10</sup> *Notice of Data Privacy Event*, *supra*, <https://www.elyriafoundry.com/media/hhucfcug/elyria-web-notice.pdf> (last visited Dec. 18, 2024).



- a. “stay alert for incidents of identity theft and fraud by reviewing your account statements and checking your free credit reports for suspicious activity and to detect errors[.]”
- b. “contact the three major credit reporting bureaus listed below to request a free copy of their credit report[.]” and
- c. “educate [yourself] regarding identity theft, fraud alerts, credit freezes, and the steps [you] can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or [your] state Attorney General.”<sup>11</sup>

39. Defendants failed their duties when their inadequate security practices caused the Data Breach. In other words, Defendants’ negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information. And thus, Defendants caused widespread injury and monetary damages.

40. Since the breach, Defendants have declared that “we made additional improvements to our network’s security[.]”<sup>12</sup>

41. But such simple declarations are insufficient to ensure that Plaintiffs’ and Class Members’ Private Information will be protected from additional exposure in a subsequent data breach.

42. Further, the Notice of Data Breach shows that Defendants cannot—or will not—determine the full scope of the Data Breach, as Defendants have been unable to determine precisely what information was stolen and when.

---

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

43. Defendants have done little to remedy their Data Breach. True, Defendants have offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class Members for the injuries that Defendants inflicted upon them.

44. Defendants had obligations created by contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

45. Plaintiffs and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

46. Defendants' data security obligations were particularly important given the frequency of cyber attacks in the manufacturing sector preceding the date of the Data Breach.

47. A 2024 study by IBM "ranked manufacturing as the most-attacked industry by cybercriminals."<sup>13</sup>

48. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industry, including Defendants.

### ***Playcrypt & the Dark Web***

49. Worryingly, the cybercriminals that obtained Plaintiffs' and Class Members' Private Information appear to be the notorious cybercriminal group "Playcrypt."<sup>14</sup>

---

<sup>13</sup> Michelle Alvarez, Industry Week, *Manufacturing Is #1 in Cyber Attacks for Third Straight Year. What Can Be Done?* (May 28, 2024), available at <https://www.industryweek.com/technology-and-iiot/cybersecurity/article/55043740/manufacturing-is-1-in-cyber-attacks-for-third-straight-year-what-can-be-done> (last visited Dec. 18, 2024).

<sup>14</sup> BreachSense, *Elyria*, <https://www.breachsense.com/breaches/elyria-foundry-data-breach/> (last visited Dec. 18, 2024).

50. Playcrypt (a.k.a., “Play Ransomware”) is an especially notorious cybercriminal group. In fact, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint report warning the public about Play Ransomware.<sup>15</sup> Specifically, the joint “Cybersecurity Advisory” (CSA) stated, *inter alia*, that:

- a. “Since June 2022, the Play (also known as Playcrypt) ransomware group has impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe.”<sup>16</sup>
- b. “The Play ransomware group is presumed to be a closed group, designed to ‘guarantee the secrecy of deals,’ according to a statement on the group’s data leak website.”<sup>17</sup>
- c. “Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data.”<sup>18</sup>
- d. “If a victim refuses to pay the ransom demand, the ransomware actors threaten to publish exfiltrated data to their leak site on the Tor network.”<sup>19</sup>

51. Here, third-party reports reveal that Playcrypt promised to ***publish*** the stolen Private Information by July 11, 2024.<sup>20</sup> A screenshot of Playcrypt’s Dark Web webpage is reproduced below.<sup>21</sup> Thus, upon information and belief, the stolen Private Information was ***already published*** on the Dark Web by Playcrypt.

---

<sup>15</sup> FBI & CISA, #StopRansomware: Play Ransomware (Dec. 18, 2023) <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a> (last visited Dec. 18, 2024).

<sup>16</sup> *Id.*

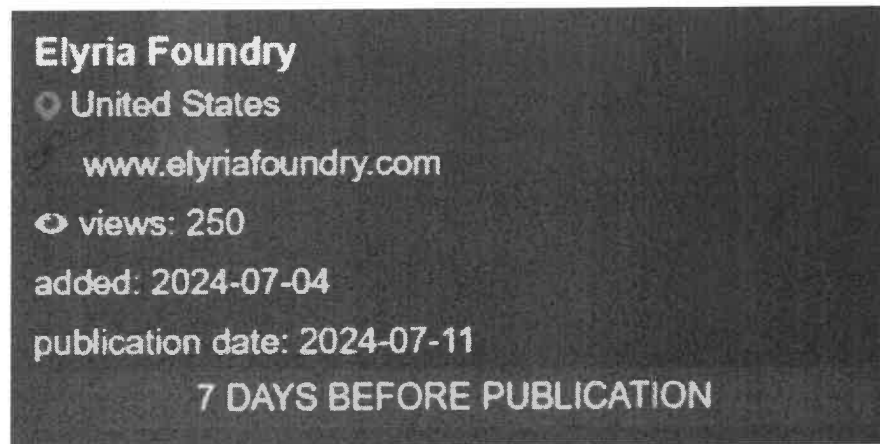
<sup>17</sup> *Id.*

<sup>18</sup> *Id.*

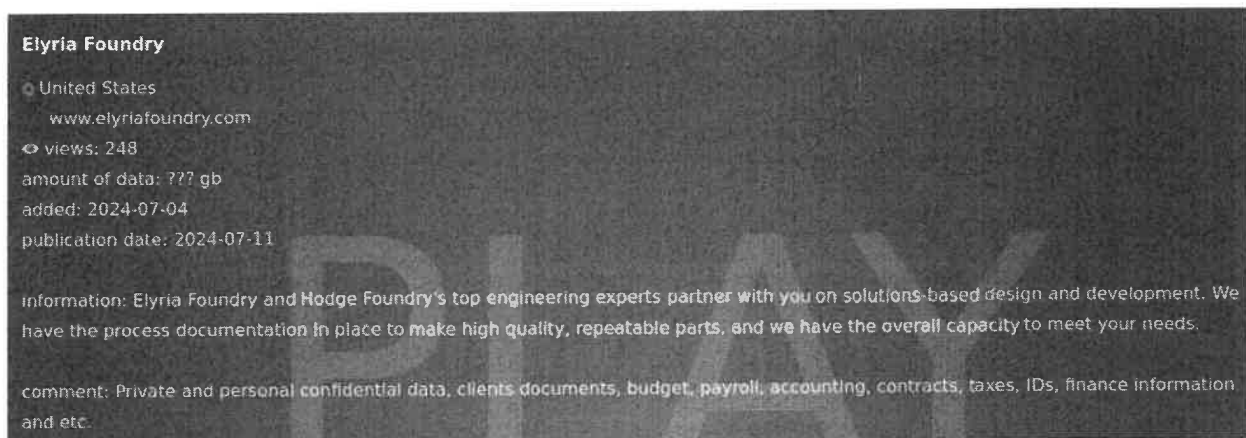
<sup>19</sup> *Id.*

<sup>20</sup> @FalconFeedsio, X (July 4, 2024, 9:50 PM), <https://x.com/FalconFeedsio/status/1809057174951284824> (last visited Dec. 18, 2024).

<sup>21</sup> *Id.*



52. Furthermore, a separate screenshot (reproduced below) reveals that the stolen Private Information includes “Private and personal confidential data, clients [*sic*] documents, budget, payroll, accounting, contracts, taxes, IDs, finance information and etc.”<sup>22</sup>



53. Thus, upon information and belief, the scope of Private Information exposed is *far greater* compared to what Defendants have disclosed thus far. Thus, upon information and belief, the exposed Private Information of Plaintiffs and Class Members includes:

- a. names;
- b. Social Security numbers;
- c. “Private and personal confidential data[;]”

<sup>22</sup> RansomLook, *Play*, <https://www.ransomlook.io/group/play> (last visited Dec. 18, 2024).

- d. “accounting” information;
- e. “contract[]” information;
- f. “tax[]” information;
- g. personal “IDs”; and
- h. “finance information.”<sup>23</sup>

54. Critically, the “views” of Playcrypt’s Dark Web website has been *steadily increasing* over time—which evidences that the Private Information of Plaintiffs and Class Members is being actively disseminated among cybercriminals on the Dark Web.

55. *First*, a screenshot seemingly from July 4, 2024, listed “246” views.<sup>24</sup>

56. *Second*, a screenshot seemingly from July 4, 2024, listed “248” views.<sup>25</sup>

57. *Third*, a screenshot seemingly from July 4, 2024, listed “250” views.<sup>26</sup>

58. *Fourth*, a third-party report from July 5, 2024, listed “384” views.<sup>27</sup>

59. Thus, upon information and belief, the Private Information of Plaintiffs and Class Members has been published—and is being actively disseminated—by cybercriminals (including Playcrypt) on the Dark Web.

#### ***Defendants Failed to Comply with FTC Guidelines***

60. The Federal Trade Commission (“FTC”) has promulgated many guides for businesses which show how important it is to implement reasonable data security practices. According to the FTC, the need for data security should shape all business decision-making.

---

<sup>23</sup> See *id.*

<sup>24</sup> @Comparitech, X (Sept. 4, 2022, 2:08 AM) <https://mobile.x.com/Comparitech/status/1831227801451597879> (last visited Oct. 21, 2024).

<sup>25</sup> RansomLook, *Play*, *supra*, <https://www.ransomlook.io/group/play>.

<sup>26</sup> @FalconFeedsio, X, *supra*, <https://x.com/FalconFeedsio/status/1809057174951284824>.

<sup>27</sup> HookPhish, *Ransomware Play Group Hits: Elyria Foundry* (July 5, 2024), <https://www.hookphish.com/blog/ransomware-play-group-hits-elyria-foundry/> (last visited Dec. 18, 2024).

61. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.<sup>28</sup> The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>29</sup>

62. The FTC further recommends that companies not maintain Private 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.

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect client 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 also clarify the measures businesses must take to meet their data security obligations.

---

<sup>28</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), available at [www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](http://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Dec. 18, 2024).

<sup>29</sup> *Id.*

64. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

65. Defendants were always fully aware of their obligation to protect the Private Information of their employees. Defendants were also aware of the significant repercussions that would result from its failure to do so.

***Defendants Failed to Comply with Industry Standards***

66. As shown above, experts studying cyber security routinely identify manufacturers as being particularly vulnerable to cyberattacks.

67. Several best practices have been identified that at a minimum should be implemented by manufacturing businesses like Defendants, including, but not limited to, educating all employees; strong passwords; multi-layer security, including firewalls, antivirus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

68. Other best cybersecurity practices that are standard in manufacturing businesses include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

69. Upon information and belief, Defendants failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01,

PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. These foregoing frameworks are existing and applicable industry standards in the manufacturing industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

## **V. DEFENDANTS' BREACH**

71. Defendants breached their obligations to Plaintiffs and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems and its data. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect employees' Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to train employees in the proper handling of emails, and to and maintain adequate email security practices;
- e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;
- f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and
- g. Failing to adhere to industry standards for cybersecurity.

72. As the result of computer systems needing security upgrading, inadequate procedures for handling emails containing ransomware or other malignant computer code, and inadequately trained employees who opened files containing malignant code, Defendants negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.



73. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft.

***Because of Defendants' Failure to Safeguard Private Information, Plaintiffs and the Class Members Have and Will Experience Substantial Harm in the Form of Risk of Continued Identity Theft.***

74. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendants.

75. The ramifications of Defendants' failure to keep Plaintiffs' and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes. According to experts, one out of four data breach notification recipients becomes a victim of identity fraud.

76. Because of Defendants' failures to prevent—and to timely detect—the Data Breach, Plaintiffs 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 Private Information is used;
- b. The diminution in value of their Private Information;
- c. The compromise and continuing publication of their Private Information;
- 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 attempting to mitigate the actual and 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 Private Information; and

h. The continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in its possession.

77. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to \$1,000.00 depending on the type of information obtained.

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

79. It can take victims years to spot identity or Private Information theft, giving criminals plenty of time to abuse that information for profit.

80. One example of criminals using Private Information for profit is the development of "Fullz" packages.

81. Cyber-criminals can cross-reference two sources of Private Information 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.

82. The development of "Fullz" packages means that stolen Private Information 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 Private Information 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 Plaintiffs and members of the proposed Class, 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 Private Information is being misused, and that such misuse is traceable to the Data Breach.

83. 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, and the numbers are only rising.

84. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good" Defendants did not rapidly report to Plaintiffs and the Class that their Private Information had been stolen.

85. 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.

86. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend considerable time repairing the damage caused by the theft of their Private Information. 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.

87. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

88. The Federal Trade Commission (“FTC”) has also 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.”<sup>30</sup>

89. According to the FTC, unauthorized Private Information disclosures ravage consumers’ finances, credit history and reputation, and can take time, money and patience to resolve the fallout.<sup>31</sup> The FTC treats 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(a) of the FTC Act.

90. Defendants’ failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs’ and Class Members’ injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

## **VI. PLAINTIFFS’ EXPERIENCE**

### ***Plaintiff Colton McClintock’s Experiences and Injuries***

91. Plaintiff Colton McClintock is and at all times mentioned herein was an individual citizen of Ohio, residing in the city of Lorain.

92. Plaintiff McClintock is a former employee of Defendants.

---

<sup>30</sup> Statement of FTC Commissioner Pamela Jones Harbour-Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), *available at* <https://www.ftc.gov/news-events/news/speeches/remarks-ftc-exploring-privacy-roundtable> (last visited Dec. 17, 2024).

<sup>31</sup> See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), *available at* <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen> (last visited Dec. 17, 2024).

93. Thus, Defendants obtained and maintained Plaintiff's Private Information. And as a result, Plaintiff was injured by Defendants' Data Breach.

94. Plaintiff received a Notice of Data Breach in October 2024.

95. As a condition of his employment with Defendants, Plaintiff provided Defendants with his Private Information. Defendants used that Private Information to facilitate their employment of Plaintiff, including payroll, and required Plaintiff to provide that Private Information in order to obtain employment and payment for that employment.

96. Plaintiff provided his Private Information to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

97. Plaintiff reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of Private Information.

98. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

99. Plaintiff is very careful about sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for online accounts containing sensitive information.

100. Plaintiff would not have provided his Private Information to Defendants had he known that Defendants would not take reasonable steps to safeguard it.

101. Thus, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

102. Through their Data Breach, Defendants compromised *at least* Plaintiff's name and Social Security number. See Plaintiff's notice letter attached as Exhibit A. However, upon information and belief, and as alleged *supra*, a far greater range of Plaintiff's Private Information was stolen in the Data Breach.

103. Plaintiff *already* suffered from identity theft and fraud—after the breach, cybercriminals stole his identity and used his Private Information to make fraudulent charges on his bank account. Plaintiff had to spend time working with the bank to remove the fraudulent charges and ultimately had to close his account and start fresh. After suffering through this ordeal, Plaintiff now must spend extra time and effort monitoring his bank accounts for any further efforts to steal his identity.

104. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendants directed Plaintiff to take those steps in their breach notice.

105. Indeed, Plaintiff has already spent time researching the Data Breach and reviewing his financial statements.

106. Plaintiff has spent much time responding to the dangers from the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including, but not limited to work and recreation.

107. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

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

109. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

110. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

111. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's Private Information right in the hands of criminals.

112. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

113. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

***Plaintiff Tanner Wolcott's Experiences and Injuries***

114. Plaintiff Tanner Wolcott is and at all times mentioned herein was an individual citizen of Pennsylvania, residing in the city of Greenville.

115. Plaintiff Tanner Wolcott is a former employee of Defendants (having worked for Defendants from approximately 2018 until 2019).

116. Thus, Defendants obtained and maintained Plaintiff's Private Information. And as a result, Plaintiff was injured by Defendants' Data Breach.

117. Plaintiff received a Notice of Data Breach dated September 3, 2024. Ex. B.

118. As a condition of his employment with Defendants, Plaintiff provided Defendants with his Private Information. Defendants used that Private Information to facilitate their employment of Plaintiff, including payroll, and required Plaintiff to provide that Private Information in order to obtain employment and payment for that employment.

119. Plaintiff provided his Private Information to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

120. Plaintiff reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of Private Information.

121. Plaintiff does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

122. Plaintiff is very careful about sharing his sensitive Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for online accounts containing sensitive information.



123. Plaintiff would not have provided his Private Information to Defendants had he known that Defendants would not take reasonable steps to safeguard it.

124. Thus, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

125. Through their Data Breach, Defendants compromised *at least* Plaintiff's name and Social Security number. Ex. B. However, upon information and belief, and as alleged *supra*, a far greater range of Plaintiff's Private Information was stolen in the Data Breach.

126. Plaintiff *already* suffered from identity theft and fraud—on June 24, 2024, cybercriminals stole his identity and used his Private Information to create a fraudulent account with “Spectrum.”

127. Additionally, in October 2024, Plaintiff suffered an unauthorized charge on his Apple card in the amount of \$149.34 for a purchase made on Amazon.

128. Further, after the Data Breach, Plaintiff has been flooded with fraudulent attempts by cybercriminals to sign into his “Venmo” and “Apple” accounts.

129. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendants directed Plaintiff to take those steps in their breach notice.

130. Indeed, Plaintiff spent approximately 5–10 hours changing his passwords, attempting to address the fraudulent Spectrum account created in his name, and filing a dispute for the fraudulent Amazon charge on his Apple account.

131. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam text messages (up to 10 times per day).

132. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

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

134. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

135. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

136. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's Private Information right in the hands of criminals.

137. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

138. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

***Plaintiff Alicia Wolcott's Experiences and Injuries***

139. Plaintiff Alicia Wolcott is and at all times mentioned herein was an individual citizen of Pennsylvania, residing in the city of Greenville.

140. Plaintiff Alicia Wolcott is the spouse of Plaintiff Tanner Wolcott.

141. Pursuant to Tanner Wolcott's employment with Defendants, Defendants obtained the Private Information of Alicia Wolcott. As a result, Plaintiff was injured by Defendants' Data Breach.

142. Plaintiff received a Notice of Data Breach in September 2024.

143. As a condition of Tanner Wolcott's employment with Defendants, Plaintiff Alicia Wolcott provided Defendants with her Private Information. Defendants used that Private Information to facilitate their provision of employment benefits to Plaintiff Alicia Wolcott.

144. In fact, Plaintiff Alicia Wolcott was required to provide her Private Information to Defendants in order to obtain employment-related benefits.

145. Plaintiff provided her Private Information to Defendants and trusted the company would use reasonable measures to protect it according to Defendants' internal policies, as well as state and federal law. Defendants obtained and continues to maintain Plaintiff's Private Information and have a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

146. Plaintiff reasonably understood that a portion of the funds paid to Defendants (and/or derived from Tanner Wolcott's employment) would be used to pay for adequate cybersecurity and protection of Private Information.

147. Plaintiff does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

148. Plaintiff is very careful about sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff also stores any documents containing her sensitive information

in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for online accounts containing sensitive information.

149. Plaintiff would not have provided her Private Information to Defendants had she known that Defendants would not take reasonable steps to safeguard it.

150. Thus, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

151. Through their Data Breach, Defendants compromised *at least* Plaintiff's name and Social Security number. However, upon information and belief, and as alleged *supra*, a far greater range of Plaintiff's Private Information was stolen in the Data Breach.

152. Plaintiff has *already* suffered from identity theft and fraud—in late June 2024, Plaintiff was informed by the IRS that someone had attempted to file her taxes using her Private Information.

153. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendants directed Plaintiff to take those steps in their breach notice.

154. Indeed, Plaintiff has already spent approximately 5–10 hours attempting to address the identity theft reported by the IRS.

155. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam text messages.

156. Plaintiff fears for her personal financial security and worries about what information was exposed in the Data Breach.

157. Because of Defendants' Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

158. Plaintiff suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

159. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendants were required to adequately protect.

160. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendants' Data Breach placed Plaintiff's Private Information right in the hands of criminals.

161. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate her injuries.

162. Today, Plaintiff has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendants' possession—is protected and safeguarded from additional breaches.

## **VII. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES**

163. To date, Defendants have done little to provide Plaintiffs and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendants have only offered 12 months of inadequate identity monitoring services, despite Plaintiffs and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

164. The 12 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity

theft and financial fraud. What's more, Defendants place the burden on Plaintiffs and Class Members by requiring them to expend time signing up for that service rather than automatically enrolling all victims of this Data Breach.

165. Defendants' credit monitoring advice to Plaintiffs and Class Members places the burden on Plaintiffs and Class Members, rather than on Defendants, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Breach.

166. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

167. Plaintiffs' Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

168. Plaintiffs were damaged in that their Private Information is in the hands of cyber criminals.

169. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

170. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have been forced to expend time dealing with the effects of the Data Breach.

171. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

172. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential

fraudsters could use that information to more effectively target such schemes to Plaintiffs and Class Members.

173. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

174. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

175. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

176. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

- a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;
- b. Purchasing credit monitoring and identity theft prevention;
- c. Placing “freezes” and “alerts” with reporting agencies;
- d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;
- e. Contacting financial institutions and closing or modifying financial accounts; and
- f. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

177. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, is protected from

further breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

178. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

### **VIII. CLASS ACTION ALLEGATIONS**

179. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Ohio Rules of Civil Procedure.

180. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

181. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

All individuals residing in the United States whose Private Information was compromised in the Data Breach discovered by Elyria in June 2024, including all those individuals who received notice of the breach.

182. Excluded from the Class are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

183. Plaintiffs reserve the right to amend or modify the class definition with greater specificity or division after having an opportunity to conduct discovery.

184. Numerosity. The Members of the Class are so numerous that joinder of all of them in a single proceeding is impracticable. The exact number of Class Members is unknown to



Plaintiffs now, but Defendants have reported to the Maine Attorney General's office that 2,193 individuals were affected by the Data Breach.

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

- a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;
- b. Whether Defendants 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 Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- d. Whether Defendants' data security systems prior to and during the Data Breach adhered to industry standards;
- e. Whether Defendants owed a duty to Class Members to safeguard their Private Information;
- f. Whether Defendants breached their duty to Class Members to safeguard their Private Information;
- g. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;
- h. Whether Plaintiffs and Class Members suffered legally cognizable damages from Defendants' misconduct;
- i. Whether Defendants were unjustly enriched;
- j. Whether Defendants failed to provide notice of the Data Breach promptly; and
- k. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

186. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, among

other things, all Class Members were injured through the common misconduct of Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and no defenses are unique to Plaintiffs. Plaintiffs' claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

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

188. Predominance. Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

189. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy.

190. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

191. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

192. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendants.

## **IX. CAUSES OF ACTION**

### **FIRST COUNT**

#### **Negligence**

#### **(On Behalf of Plaintiffs and All Class Members)**

193. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

194. Defendants required Plaintiffs and Class Members to submit non-public personal information to be considered for employment at Elyria.

195. Plaintiffs and the Class (or their third-party agents) entrusted their Private Information to Defendants on the premise and with the understanding that Defendants would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

196. By collecting and storing this data in Defendants' computer property, and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information held within—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

197. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

198. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

199. Defendants' duty of care to use reasonable security measures arose because of the special relationship that existed between Defendants and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential Private Information, a necessary part of obtaining employment from Defendants.

200. Defendants owed—to Plaintiffs and Class Members—at least the following duties to:

- a. exercise reasonable care in handling and using the Private Information in their care and custody;
- b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;
- c. promptly detect attempts at unauthorized access;
- d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

201. Thus, Defendants owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their

Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

202. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

203. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

204. Defendants further had a duty to use reasonable care in protecting confidential data because Defendants are bound by industry standards to protect confidential Private Information.

205. Defendants breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members’ Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members’ Private Information;
- b. Failing to adequately monitor the security of its networks and systems;
- c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members’ Private Information;
- e. Failing to detect timely that Class Members’ Private Information had been compromised;
- f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- g. Failing to secure its stand-alone personal computers, such as reception desk computers, even after discovery of the data breach.

206. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the manufacturing industry.

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

208. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by:

- a. disclosing and providing access to this information to third parties and
- b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

209. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and Private Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs and Class Members' injury.

210. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class Members' injuries-in-fact.

211. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

212. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

213. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

214. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

215. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

216. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

**SECOND COUNT**  
**Breach of Implied Contract**  
**(On Behalf of Plaintiffs and All Class Members)**

217. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

218. Plaintiff and Class Members either directly contracted with Defendants or Plaintiff and Class Members were the third-party beneficiaries of contracts with Defendants.

219. When Plaintiffs and Class Members (or their third-party agents) provided their Private Information to Defendants in exchange for consideration for employment, they entered implied contracts with Defendants under which Defendants agreed to reasonably protect such information.

220. Defendants required Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

221. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and adhered to industry standards.

222. Plaintiffs and Class Members provided labor to Defendants with the reasonable belief and expectation that Defendants would use part of their earnings to obtain adequate data security. Defendants failed to do so.

223. In turn, and through internal policies, Defendants agreed to protect and not disclose the Private Information to unauthorized persons.

224. In their Privacy Policy, Defendants represented that they had a legal duty to protect Plaintiffs' and Class Member's Private Information.

225. Implicit in the parties' agreement was that Defendants would provide Plaintiffs and Class Members (or their third-party agents) with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

226. After all, Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

227. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.



228. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

229. Defendants breached their implied contracts with Class Members by failing to safeguard and protect their Private Information.

230. As a direct and proximate result of Defendants' breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

231. The covenant of good faith and fair dealing is an element of every contract. Thus, 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—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

233. Defendants materially breached the contracts they entered with Plaintiffs and Class Members (or their third-party agents) by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into their computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

- e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendants created, received, maintained, and transmitted.

234. In these and other ways, Defendants violated their duty of good faith and fair dealing.

235. Defendants' material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

236. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

237. Plaintiffs and Class Members (or their third-party agents) performed as required under the relevant agreements, or such performance was waived by Defendants' conduct.

238. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

239. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

**THIRD COUNT**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs and All Class Members)**

240. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

241. This claim is pleaded in the alternative to the breach of implied contract claim.

242. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is pled in the alternative to the breach of contract count above.

243. Upon information and belief, Defendants fund its data security measures entirely from its general revenue.

244. As such, a portion of the revenue attributable to Plaintiffs' and Class Members' labor is to be used to provide a reasonable level of data security.

245. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Plaintiffs and Class Members (or their third-party agents) conferred a benefit upon Defendants. After all, Defendants benefitted from (1) using their Private Information to facilitate employment, and (2) using their labor to derive profit.

246. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

247. Plaintiffs and Class Members (or their third-party agents) reasonably understood that Defendants would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendants' duties under state and federal law and their internal policies.

248. Defendants enriched themselves by saving the costs Defendants reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Rather than providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by using cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize its own profits over the requisite security.

249. Under the principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs' and Class Members' (1) Private Information and (2) employment because Defendants failed to adequately protect their Private Information. Defendants

failed to secure Plaintiffs' and Class Members' Private Information and thus did not provide full compensation for the benefit Plaintiffs and Class Members provided.

250. Defendants acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices alleged.

251. If Plaintiffs and Class Members knew that Defendants had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

252. Plaintiffs and Class Members have no adequate remedy at law.

253. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

- a. actual identity theft;
- b. the loss of the opportunity to control how their Private Information is used;
- c. the compromise, publication, and/or theft of their Private Information;
- d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;
- e. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;
- f. the continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and
- g. future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiffs and Class Members.

254. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

255. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them.

**FOURTH COUNT**  
**Invasion of Privacy**  
**(On Behalf of Plaintiffs and the Class)**

256. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

257. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

258. Defendants owed a duty to their current and former employees (and their spouses and dependents), including Plaintiffs and the Class, to keep this information confidential.

259. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class Members' Private Information is highly offensive to a reasonable person.

260. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendants, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

261. The Data Breach constitutes an intentional interference with Plaintiffs' 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.

262. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

263. Defendants acted with a knowing state of mind when they failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

264. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

265. As a proximate result of Defendants' acts and omissions, the private and sensitive Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

266. And, on information and belief, Plaintiffs' Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

267. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their Private Information are still maintained by Defendants with their inadequate cybersecurity system and policies.

268. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the Private Information of Plaintiffs and the Class.

269. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class Members, also seek compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

**FIFTH COUNT**  
**Declaratory Judgment**  
**(On Behalf of Plaintiffs and All Class Members)**

270. Plaintiffs re-allege and incorporate the above allegations as if fully set forth herein.

271. Under the Ohio Declaratory Judgments Act, O.R.C. § 2721.01, *et seq.*, this Court may enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

272. Defendants owe a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

273. Defendants still possess Private Information about Plaintiffs and Class Members.

274. Plaintiffs allege that Defendants' data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury because of the compromise of their Private Information and the risk remains that further compromises of their Private Information will recur.

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

- a. Defendants owe a legal duty to secure their employees' Private Information and to timely notify them of a data breach under the common law and the FTCA;
- b. Defendants' existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect their employees' Private Information; and
- c. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure its employees' Private Information.

276. This Court should also issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with legal and industry standards to protect its employees' Private Information, including the following:

- a. Order Defendants to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.
- b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:
  - i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems periodically, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
  - ii. engaging third-party security auditors and internal personnel to run automated security monitoring;
  - iii. auditing, testing, and training its security personnel regarding any new or modified procedures;
  - iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;
  - v. conducting regular database scanning and security checks;
  - vi. 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; and
  - vii. meaningfully educating its employees about the threats faced regarding the security of their Private Information.

277. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Elyria occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

278. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and related damages if an injunction is not issued. On the other hand, the cost of



Defendants' compliance with an injunction requiring reasonable prospective data security measures is minimal, and Defendants have a preexisting legal obligation to employ such measures.

279. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendants, thus preventing future injury to Plaintiffs and other employees whose Private Information would be further compromised.

#### **X. PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above seek the following relief:

- a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiffs and their counsel to represent the Class, and finding that Plaintiffs are proper representatives of the Class requested herein;
- b. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;
- c. For equitable relief compelling Defendants to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;
- d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendants' wrongful conduct;
- e. For an Order directing Defendants to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;
- f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- g. For an award of punitive damages, as allowable by law;
- h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;
- i. Pre- and post-judgment interest on any amounts awarded; and
- j. Any other relief that this court may deem just and proper.

**XI. JURY TRIAL DEMANDED**

Plaintiffs demand a trial by jury on all claims so triable.

Dated: January 13, 2024



---

Robert E. DeRose (OH Bar No. 0055214)  
**BARKAN MEIZLISH DEROSE COX, LLP**  
4200 Regent Street, Ste. 210  
Columbus, OH 43219  
Phone: (614) 221-4221  
Facsimile: (614) 744-2300  
bderose@barkanmeizlish.com

Leigh S. Montgomery (*pro hac vice*)  
Texas Bar No. 24052214  
lmontgomery@eksm.com  
**EKSM, LLP**  
1105 Milford Street  
Houston, Texas 77006  
Phone: (888) 350-3931  
Fax: (888) 276-3455

Samuel J. Strauss\*  
Raina C. Borrelli\*  
**STRAUSS BORRELLI PLLC**  
980 N. Michigan Avenue, Suite 1610  
Chicago, Illinois 60611  
T: (872) 263-1100  
F: (872) 263-1109  
sam@straussborrelli.com  
raina@straussborrelli.com

*\*Pro hac vice forthcoming*

*Attorneys for Plaintiffs and the Proposed Class*


**CERTIFICATE OF SERVICE**

I certify that on January 13, 2025, the foregoing Amended Complaint has been served on counsel for Defendant via regular, prepaid US Mail.

Thomas Moran  
Mullen Coughlin LLC  
70 Birch Alley, Suite 240  
Beavercreek, OH 45440

Paulyne A. Gardner\*  
Carolyn Purwin Ryan\*  
Mullen Coughlin LLC  
426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

*Attorneys for Defendant*

  
Robert E. DeRose

*Counsel for Plaintiffs*

## **EXHIBIT A**



Return mail will be processed by: ISC  
PO Box 647 • Holbrook, NY 11741

COLTON MCCLINTOCK  
[Redacted Address]

September 3, 2024

## NOTICE OF SECURITY INCIDENT

Dear Colton McClintock:

Elyria Foundry Holdings LLC is writing to notify you of a recent incident that may have affected the privacy of some of your personal information. This incident affected our Elyria Foundry and Hodge Foundry locations. Even though we have no evidence of any fraudulent misuse of your personal information, we want to tell you about the incident, our response, and steps you can take to help protect your information, should you decide to do so.

**What Happened?** On June 25, 2024, we became aware of suspicious activity in our computer network. We quickly secured our network and hired outside specialists to help us investigate. The investigation found that for a few hours between June 24, 2024, and June 25, 2024, an unknown actor accessed part of our network and may have viewed and/or copied some of our files. In response, we reviewed the affected files to identify whether those files contained any personal information. Our review found that information about current and former employees and their spouses and dependents may have been impacted by this incident.

**What Information Was Involved?** Your name and Social Security number may have been present in the affected files. The investigation did not confirm whether your information was actually viewed or taken, but we cannot rule out this possibility. We have no indication of identity theft or fraud related to this incident.

**What We Are Doing.** The confidentiality, privacy, and security of personal information are among our highest priorities. Before this incident happened, we already had advanced security measures in place to protect our systems and information. After we became aware of this incident, we made additional improvements to our network's security to help prevent this from happening again in the future.

Additionally, we are offering credit monitoring and identity protection services for 12 months through CyberScout, a TransUnion company specializing in fraud assistance and remediation services, at no cost to you. Please note that you will not be automatically enrolled in these services and we are not able to enroll on your behalf. Instructions on how to enroll in these services is in the enclosed *Steps You Can Take to Help Protect Personal Information*.

**What You Can Do.** In addition, we encourage you to stay alert for incidents of identity theft and fraud by reviewing your account statements and checking your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.

# **Exhibit B**

ELYRIA EF FOUNDRY



Hodge Foundry

Return mail only to be provided by: BFC  
PO Box 847 • Holbrook, NY 11741

TANNER WOLCOTT

September 3, 2024

## NOTICE OF SECURITY INCIDENT

Dear Tanner Wolcott:

Elyria Foundry Holdings LLC is writing to notify you of a recent incident that may have affected the privacy of some of your personal information. This incident affected our Elyria Foundry and Hodge Foundry locations. Even though we have no evidence of any fraudulent misuse of your personal information, we want to tell you about the incident, our response, and steps you can take to help protect your information, should you decide to do so.

**What Happened?** On June 25, 2024, we became aware of suspicious activity in our computer network. We quickly secured our network and hired outside specialists to help us investigate. The investigation found that for a few hours between June 24, 2024, and June 25, 2024, an unknown actor accessed part of our network and may have viewed and/or copied some of our files. In response, we reviewed the affected files to identify whether those files contained any personal information. Our review found that information about current and former employees and their spouses and dependents may have been impacted by this incident.

**What Information Was Involved?** Your name and Social Security number may have been present in the affected files. The investigation did not confirm whether your information was actually viewed or taken, but we cannot rule out this possibility. We have no indication of identity theft or fraud related to this incident.

**What We Are Doing.** The confidentiality, privacy, and security of personal information are among our highest priorities. Before this incident happened, we already had advanced security measures in place to protect our systems and information. After we became aware of this incident, we made additional improvements to our network's security to help prevent this from happening again in the future.

Additionally, we are offering credit monitoring and identity protection services for 12 months through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services, at no cost to you. Please note that you will not be automatically enrolled in these services and we are not able to enroll on your behalf. Instructions on how to enroll in these services is in the enclosed *Steps You Can Take to Help Protect Personal Information*.

**What You Can Do.** In addition, we encourage you to stay alert for incidents of identity theft and fraud by reviewing your account statements and checking your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information*.