**IN THE UNITED STATES DISTRICT COURT**
**FOR THE EASTERN DISTRICT OF PENNSYLVANNIA**

| | | |
|---|---|---|
| TARA ADAMEK, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>FIREWORKS SOFTWARE, INC.,<br><br>Defendant. | ) | **Case No.: 2:24-cv-5185**<br><br>**JURY TRIAL DEMANDED** |

## CLASS ACTION COMPLAINT

Plaintiff Tara Adamek ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Fireworks Software, Inc. ("Fireworks Software" or "Defendant").

## NATURE OF THE ACTION

1. This is a class action for damages with respect to Fireworks Software for its failure to exercise reasonable care in securing and safeguarding users' sensitive information—including full names, dates of birth, Social Security numbers, and alien registration numbers, collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of individual's who received a notice letter from Fireworks Software and had their sensitive PII accessed by unauthorized parties because of a lapse in network security in or around June of 2024 (the "Data Breach").

3. The Data Breach affected thousands of customers. Furthermore, the Data Breach could have been prevented had Fireworks Software implemented adequate data security protocols, practices, and procedures. It failed to do so.

4. Fireworks Software reported to Plaintiff that the information compromised in the Data Breach included her PII, but such notification did not occur until September 17, 2024 – nearly three months after her Private Information was first accessed.

5. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant that was compromised in and as a result of the Data Breach.

6. Plaintiff also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling her PII.

7. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

8. As a result of the Data Breach, Plaintiff and other members of the "Class" (defined below) will continue to experience and/or are at an imminent and substantial risk of experiencing various types of misuse of their PII, including but not limited to, spam calls and emails, unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their PII.

9. There has been no assurance offered from Fireworks Software that all personal data or copies of data have been recovered or destroyed, or that it has implemented adequate data security protocols, practices, and procedures necessary to prevent a similar data breach in the future. Fireworks Software offered Plaintiff and the Class only twelve (12) months of Cyberscout credit monitoring, which is woefully inadequate considering the imminent and substantial risk of harm they now face.

10. Accordingly, Plaintiff asserts claims for negligence, breach of implied contract, and statutory consumer protection violations and seeks injunctive relief, monetary damages, statutory damages, and any other relief as authorized by the Court in equity or by law, and does so on behalf of herself and the Class.

## PARTIES

### A. Plaintiff Tara Adamek

11. Plaintiff Tara Adamek is a resident of Cherry Hill, New Jersey and brings this action in her individual capacity and on behalf of all others similarly situated.

12. Plaintiff is a student of Rowan College. Plaintiff Adamek began taking classes with Rowan College in the spring of 2022, however she took a placement test prior to this in June of 2021. Rowan College works with Fireworks Software for customer relationship software to maintain student records. As such, Plaintiff was required to entrust her Private Information with Fireworks Software. In maintaining this Private Information, Defendant expressly and impliedly promised to safeguard it from unauthorized access and disclosure. Defendant, however, failed in this regard and Plaintiff's Private Information was compromised as a direct result of Defendant's inadequate security measures.

13. In September of 2024, months after the Data Breach, Plaintiff Adamek received a notification letter from Defendant, informing her that her full name, Social Security number ("SSN"), and address had all been compromised, as well as potentially other data.

14. Plaintiff Adamek has already received notification from Discover and CreditWise that her Social Security Number has been found on the dark web.

15. The letter also offered only one year of credit monitoring through Cyberscout, which was and continues to be ineffective for Plaintiff and Class members.

16. In the months and years following the Data Breach, Ms. Adamek and Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms may include fraudulent charges, fraudulent accounts opened in their names, and targeted advertising without consent.

17. Plaintiff Adamek greatly values her privacy, especially in the administration of her finances, and would not have paid the amount that she did for Defendant's services had she known that her Private Information would be maintained using inadequate data security systems.

**B. Defendant**

18. Defendant is a Pennsylvania corporation, primarily engaged in the business of providing customer relationship management software. Fireworks Software's principal place of business is at 224 Lansdowne Ave, Wayne, PA 19067.

19. Fireworks Software's corporate policies and practices, including those used for data privacy, are established in, and emanate from the commonwealth of Pennsylvania.

## JURISDICTION AND VENUE

20. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

21. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

22. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the

Class's claims also occurred in this District.

**FACTS**

23. Defendant provides customer relationship management software to colleges throughout Pennsylvania and the United States. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect, the Private Information of Plaintiff and the Class in accordance with all applicable law and industry standards.

24. In June of 2024, Defendant first learned of unauthorized access to its network, allowing hackers to gain access to customers' Private Information, including names, dates of birth, and Social Security numbers.

25. Fireworks Software's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how the unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the Breach occurred system-wide, whether servers storing information were accessed, and how many customers were affected by the Data Breach.

26. Even worse, Fireworks Software offered only one year of identity monitoring for Plaintiff and Class members, requiring disclosure of additional PII with which Fireworks Software had just demonstrated it could not be trusted.

27. Plaintiff's and Class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and Class members' unencrypted, unredacted Private Information.

28. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this release of information, despite repeated

warnings to the educational sector about the risk of inadequate data security measures in securing consumers' personal information.

29. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was compromised through unauthorized access. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

**A. Defendant's Privacy Promises**

30. Fireworks Software made, and continues to make, various promises to its customers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

31. Defendant previously stated on its website that "Fireworks, the software division of Fire Engine RED, is committed to the privacy of client and end-user information. We will never sell, rent, or share data hosted on behalf of our clients unless we are given permission or compelled by court order to do so."[1]

**B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Students' and Employees' PII**

32. Fireworks Software acquires, collects, and stores a massive amount of PII from

[1] https://web.archive.org/web/20231205051430/https://www.fireworkssoftware.com/privacy-policy/ (Fireworks Software appears to have since shut down its website in anticipation of suspending operations) (captured on 12/5/2023).

students, applicants, and employees of the various colleges that is services.

33. As a condition of engaging in student or applicant services and/or employment with various colleges, Defendant requires that these students and employees entrust them with highly confidential PII.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' PII, Fireworks Software assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' PII from disclosure.

35. Defendant had obligations created by industry standards, the Family Educational Rights and Privacy Act ("FERPA"), common law, and representations made to Class members, to keep Class members' PII confidential and to protect it from unauthorized access and disclosure.

36. Defendant failed to properly safeguard Class members' PII, allowing hackers to access their PII.

37. Plaintiff and Class members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

38. Before, during, and after the Data Breach, Defendant promised students and employees that their PII would be kept confidential.

39. Defendant's failure to provide adequate security measures to safeguard student and employee PII is especially egregious because Defendant was aware that educational institutions storing sensitive PII have been frequent targets of scammers attempting to fraudulently gain access to highly confidential PII belonging to students, applicants, and employees.

40. In fact, Defendant has been on notice for years that companies who store sensitive PII are a prime target for scammers because of the amount of confidential student and employee information maintained.

41. Defendant was also on notice that data breaches have been on the rise at educational institutions. The FBI has repeatedly warned companies within the education industry that hackers were targeting them. In March of 2021, for example, the FBI's Cyber Division issued a warning stating that "unidentified cyber actors have specifically targeted higher education, K-12 schools, and seminaries. These actors use ransomware to exfiltrate data from victims prior to encrypting victim's systems to use as leverage in eliciting ransom payments."[2]

42. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[3] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[4] That trend continues.

43. Data breaches related to educational institutions continued to rapidly increase into 2024 when Fireworks Software was breached.[5]

44. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[6]

---

[2] Federal Bureau of Investigation—Cyber Division, *Increase in PYSA Ransomware Targeting Education Institutions*, (Mar. 16, 2021), https://www.ic3.gov/Media/News/2021/210316.pdf.

[3] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[4] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/ (last accessed 9/27/2024).

[5] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey (last accessed 9/27/2024).

[6] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed 9/27/2024).

45. To prevent and detect cyberattacks, including the cyberattacks that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware

locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

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

46. To prevent and detect cyberattacks, including the cyberattacks that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

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

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

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

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

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

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[7]

47. To prevent and detect cyberattacks, including the cyberattacks that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials

- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

[7] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[8]

48. These are basic, common-sense email security measures. Defendant, with its heightened standard of care, should be doing even more. By taking these commercially reasonable, common-sense steps, Fireworks Software could have prevented the Data Breach from occurring.

49. Charged with handling sensitive PII including Social Security numbers, Fireworks Software knew, or should have known, the importance of safeguarding students' and employees' PII that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on students and employees as a result of a breach. Fireworks Software failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

50. The PII was also maintained on Defendant's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's systems through

[8] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

ransomware attacks. The potential for cyberattacks and the resultant improper disclosure of Plaintiff's and Class members' PII was a known risk to Defendant, and thus Fireworks Software was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

**C. The Monetary Value of Privacy Protections and PII**

51. The fact that Plaintiff's and Class members' PII was stolen—and is being trafficked on the Dark Web—demonstrates the monetary value of the PII.

52. At all relevant times, Defendant was well aware that PII it collects from Plaintiff and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

53. PII is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and financial fraud.[9] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive information on multiple underground Internet websites, commonly referred to as the dark web.

54. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third-party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[10]

---

[9] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[10] *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

55. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[11]

56. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbor, underscored this point:

> 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. The larger the data set, the greater potential for analysis—and profit.[12]

57. Recognizing the high value that consumers place on their PII, many companies now offer consumers an opportunity to sell this information.[13] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their PII. This business has created a new market for the sale and purchase of this valuable data.

58. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and

---

[11] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[12] *Statement of FTC Commissioner Pamela Jones Harbor—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[13] *Web's Hot New Commodity*, *supra* note 11.

the amount is considerable. Indeed, studies confirm that the average direct monetary loss for victims of identity theft in 2014 was $1,349.[14]

59. The value of Plaintiff's and Class members' PII on the black market is substantial. Sensitive consumer information can sell for hundreds of dollars. It can be used to create fake insurance claims, take out loans in a person's name, or request government services that an individual is unaware of.

60. The ramifications of Defendant's failure to keep students', employees', and applicants' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

61. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[15] This gives thieves ample time to perpetrate multiple fraudulent purchases under the victim's name.

62. At all relevant times, Defendant was aware, or reasonably should have been aware, that the PII it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting educational institutions and affiliates.

63. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would

[14] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[15] *See Medical ID Theft Checklist*, IDENTITYFORCE, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last accessed 9/27/2024).

have prevented the cyberattack into its systems and, ultimately, the theft of its students', applicants' and employees' PII.

64. The PII compromised in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[16] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[17] Based upon information and belief, the unauthorized parties utilized the PII they obtained through the Data Breach to obtain additional information from Plaintiff and Class members that was misused.

65. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

66. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information was not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class members' PII to access accounts, including, but not limited to email accounts and financial accounts, to engage in fraudulent activity.

---

[16] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[17] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

67. In short, the PII exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

**D. Fireworks Software's Conduct violated FTC Standards**

68. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[18]

69. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[19] The guidelines note that businesses should protect the personal customer 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.

70. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[20]

---

[18] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[19] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[20] *Start with Security*, *supra* note 18.

71. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

72. Fireworks Software was fully aware of its obligation to protect the PII of its students and employees because of its position as an educational institution and employer. Fireworks Software was also aware of the significant repercussions that would result from its failure to do so.

**E. Damages to Plaintiff and the Class**

73. Plaintiff and the Class have been damaged by the compromise of their PII in the Data Breach.

74. The ramifications of Defendant's failure to keep students' and employees' PII secure are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[21]

75. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect PII entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in

[21] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

76. Defendant further owed and breached its duty to Plaintiff and Class members to notify past and present students, applicants, and employees affected by the Data Breach in a timely manner.

77. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff and Class members' PII as detailed above, and Plaintiff is now at a heightened and increased risk of identity theft and fraud.

78. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing, or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

79. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, services billed in their name, and similar identity theft.

80. Plaintiff and Class members have, may have, and/or will have incurred 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.

81. Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with

Defendant. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

82. Plaintiff and Class members would not have given their information to Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their PII from theft.

83. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

84. The theft of Social Security Numbers is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[22] The SSA has stated that "[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought."[23] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[24]

85. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not

[22] *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.
[23] *Id.*
[24] *Id.*

associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[25]

86. Identity thieves can use the victim's PII to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. PII can also be used to submit false insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their PII and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. PII is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

87. As a result of the Data Breach, Plaintiff's and Class members' PII has diminished in value.

88. The PII belonging to Plaintiff and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class members' consent to disclose such PII to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiff and the Class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

89. The Data Breach were a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical

[25] *Id.*

safeguards to ensure the security and confidentiality of Plaintiff and Class members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

90. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect student, applicant, and employee data.

91. Defendant did not properly train their employees to identify and avoid cyberattacks.

92. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusion into its systems and, ultimately, the theft of Plaintiff's and Class members' PII.

93. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to others life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

94. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[26]

95. Defendant's failure to adequately protect Plaintiff's and Class members' PII has resulted in Plaintiff and Class members having to undertake credit monitoring investigations into

[26] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

their own finances, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money.

96. To mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

97. While some harm has begun already, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when PII is *acquired* by criminals and when it is *used* by them. Furthermore, identity monitoring programs only alert someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's PII) – it does not prevent identity theft.[27]

98. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their PII. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and Class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and Class members also suffered a loss of the inherent value of their PII.

99. The PII stolen in the Data Breach can be misused on its own, or it can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft.

[27] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

Thieves can also use the stolen PII to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the target might agree to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

100. As a result of Defendant's failures to prevent the Breach, Plaintiff and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their PII;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- The continued risk to their PII, which remains in the possession of Defendant and is subject to further Breach so long as Defendant fails to undertake appropriate measures to protect the PII in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members; and
- Anxiety and distress resulting from fear of misuse of their PII.

101. In addition to a remedy for the economic harm, Plaintiff and Class members maintain an undeniable interest in ensuring that their PII remains secure and is not subject to further misappropriation and theft.

## CLASS ACTION ALLEGATIONS

102. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

103. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23(b)(1), (b)(2), (b)(3) and/or (c)(4).

104. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Nationwide Class and New Jersey Subclass (collectively defined herein as the "Class"):

**Nationwide Class**

> All persons nationwide whose Private Information was compromised as a result of the Data Breach discovered around June of 2024 and who were sent notice of the Data Breach.

**New Jersey Subclass**

> All citizens of New Jersey whose Private Information was compromised as a result of the Data Breach discovered around June of 2024 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

105. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

106. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the tens of thousands.

107. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and

- Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

108. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

109. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

110. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because her interests do not conflict with the interests of the Class she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and she will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

111. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23 (b)(2).

112. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The

damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

113. Alternatively, to the extent the Court determines that Rule 23(b)(2) or Rule 23(b)(3) certification is not appropriate, the Court may certify a Rule 23(c)(4) issues class for determination of common material fact issues in the case, and/or liability.

**COUNT I**
**Negligence**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New Jersey Subclass)**

114. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

115. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in its computer systems and on its networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should have been protected as such.

116. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

117. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

118. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information.

119. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

120. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

121. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

122. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' Private Information.

123. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

124. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including, but not limited to, the common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

125. In addition, Defendant 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.

126. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

127. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class member's Private Information; (2) comply with industry standard

security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

128. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to detect in a timely manner that Class members' Private Information had been compromised; and
- 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

129. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

130. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information

and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

131. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

132. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

133. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide at least five (5) years of free credit and identity theft monitoring to all Class members.

## COUNT II
## Breach of Implied Contract
## (On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New Jersey Subclass)

134. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

135. Plaintiff brings this claim alternatively to her claim for breach of contract.

136. Through its course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information.

137. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into the services agreement with Defendant.

138. The valid and enforceable implied contracts with Defendant included Defendant's implied promise to protect Plaintiff's and Class members' nonpublic Private Information given to Defendant.

139. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

140. Defendant solicited and invited Plaintiff and Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

141. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

142. Class members reasonably believed and expected that Defendant would use part of the funds paid to it by Plaintiff and Class members to obtain adequate data security. Defendant failed to do so.

143. Under implied contracts, Defendant promised and was obligated to: (a) provide services to Plaintiff and Class members; and (b) protect Plaintiff's and the Class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and members of the Class agreed to pay money for these services, and to turn over their Private Information to Defendant.

144. Both the provision of services and the protection of Plaintiff's and Class members' Private Information were material aspects of these implied contracts.

145. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, also memorialize and embody the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff's and Class members' Private Information.

146. Consumers of educational services value their privacy and the ability to keep their Private Information associated with obtaining such services safe from unauthorized access and compromise. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

147. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant and paid for the provided services in exchange for, amongst other things, both the provision of software services and the protection of their Private Information.

148. Plaintiff and Class members performed their obligations under these implied contracts by providing their Private Information to Defendant.

149. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

150. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the

privacy of Plaintiff's and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class members' Private Information as set forth above.

151. The Data Breach was a reasonably foreseeable consequence of Defendant's actions and inactions in breach of these contracts.

152. As a result of Defendant's failure to fulfill the data security protections promised, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received software and other services that were of a diminished value to that to which Defendant was contractually obligated. Plaintiff and Class members therefore were damaged in an amount at least equal to the difference in the value of the software services *with* data security protection and the actual services they received.

153. Had Defendant disclosed that its data security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have utilized services from Defendant.

154. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

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

156. Plaintiff and Class members are also entitled to injunctive relief requiring

Defendant to, *e.g.,* (i) strengthen its 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.

**COUNT III**
**Unjust Enrichment/Quasi-Contract**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New Jersey Subclass)**

157. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

158. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased software services from Defendant and provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the software services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

159. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from Plaintiff's business and used Plaintiff's and Class member's Private Information for business purposes.

160. Defendant failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff's and Class members' Private Information provided.

161. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate data security practices previously alleged.

162. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate data security, they would not have used Defendant's services.

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

164. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

165. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and the Class members overpaid for the use of Defendant's services.

**COUNT IV**
**Violations of the New Jersey Consumer Fraud Act N.J. Stat. §§ 56:8-1 *et seq.* ("NJCFA")**
**(On Behalf of Plaintiff and the New Jersey Sub-Class))**

166. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

167. This claim is brought by the Plaintiff individually and on behalf of the New Jersey Sub-Class against Fireworks Software.

168. The NJCFA states:

> The act, use or employment by any person of any commercial practice that is unconscionable or abusive, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice.
>
> N.J. Stat. § 56:8-2.

169. Plaintiff, New Jersey Sub-Class Members, and Defendant are "persons" under the NJCFA. N.J. Stat. § 56:8-1(d). 170. The services that Fireworks Software provided are "merchandise" pursuant to the NJCFA. N.J. Stat. § 56:8-1(c).

170. Fireworks Software committed deceptive omissions in violation of the NJCFA by failing to inform Plaintiff and New Jersey Sub-Class Members that they would not adequately secure Plaintiff's and New Jersey Sub-Class Members' Private Information.

171. Fireworks Software engaged in unfair acts and practices in violation of the NJCFA by failing to implement and maintain reasonable security measures to protect and secure Plaintiff's and New Jersey Sub-Class Members' Private Information in a manner that complied with applicable laws, regulations, and industry standards. The failure to implement and maintain reasonable data security measures for Private Information offends established public policy, is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

172. Due to the Data Breach, Plaintiff and New Jersey Sub-Class Members have lost property in the form of their Private Information. Further, Fireworks Software's failure to adopt reasonable practices in protecting and safeguarding patients' Private Information will force Plaintiff and New Jersey Sub-Class Members to spend time or money to protect against identity theft.

173. Plaintiff and New Jersey Sub-Class Members are now at a substantially higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Fireworks' practice of collecting and storing Private Information without appropriate and reasonable safeguards to protect such information.

174. Plaintiff and all other New Jersey Sub-Class Members were damaged by Fireworks Software's violation of the NJCFA because: (i) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their Private Information was improperly disclosed to unauthorized individuals; (iii) the confidentiality of their Private Information has been breached;

(iv) they were deprived of the value of their Private Information, for which there is a well-established national and international market; and (v) they lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

**COUNT VI**
**Declaratory/Injunctive Relief**
**(On Behalf of Plaintiff and the Nationwide Class or, Alternatively, the New Jersey Subclass)**

175. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

176. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

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

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

179. Defendant still possesses the PII of Plaintiff and the Class.

180. To Plaintiff's knowledge, Defendant has made little, if any, changes to its data storage or security practices relating to the security of the PII.

181. To Plaintiff's knowledge, Defendant has not adequately remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

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

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

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

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

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

b. auditing, testing, and training its security personnel and employees regarding any new or modified procedures;

c. purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

d. conducting regular database scans and security checks; and

e. routinely and continually conducting internal employee training and education to inform internal security personnel and employees how to prevent or detect a similar data breach when it occurs and what to do in response to such a breach.

**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury of all claims so triable.

**REQUEST FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in her favor and against Defendant, as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than five (5) years of credit monitoring services for Plaintiff 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 such other and further relief as this court may deem just and proper.

Date: September 27, 2024

Respectfully submitted,

*/s/ Gary F. Lynch*
Gary F. Lynch (PA ID No. 56887)
Patrick D. Donathen (PA ID No. 330416)
**LYNCH CARPENTER LLP**
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
patrick@lcllp.com

Nicholas A. Migliaccio*
*nmigliaccio@classlawdc.com*
Jason S. Rathod*
*jrathod@classlawdc.com*
**Migliaccio & Rathod LLP**
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

*Counsel for Plaintiff and the Putative Class*
**Pro Hac Vice* Anticipated

# ClassAction.org