



<p><b>KEVIN W. FAY, ESQUIRE</b>  <b>GOLOMB SPIRT, P.C.</b>  Identification No.: 308252  <a href="mailto:kfay@golomblegal.com">kfay@golomblegal.com</a>  1835 Market Street, Suite 2900  Philadelphia, PA 19104  (215) 985-9177</p> <p>Charles E. Shaffer (PA # 76259)  <b>LEVIN SEDRAN &amp; BERMAN</b>  510 Walnut Street, Ste. 500  Philadelphia, PA 19106  Tel: (215) 592-1500  Email: <a href="mailto:cschaffer@lfsblaw.com">cschaffer@lfsblaw.com</a></p>	<p><b>MAJOR JURY CASE</b></p> <p><b>CLASS ACTION</b>  ASSESSMENT OF DAMAGES HEARING IS  REQUIRED</p> <p><b>Attorneys for Plaintiffs and the Class</b></p>
<p><b>STEVEN HASSELL and JEROME RANIELL, individually and on behalf of all others similarly situated,</b></p> <p><b>Plaintiffs,</b></p> <p><b>v.</b></p> <p><b>SPEAR WILDERMAN, P.C.</b></p> <p><b>Defendant.</b></p>	<p><b>COURT OF COMMON PLEAS OF PHILADELPHIA COUNTY</b></p> <p><b>CIVIL ACTION -- CLASS ACTION</b>  <b>JURY TRIAL DEMANDED</b></p> <p><b>No: 230401942</b></p>

**FIRST AMENDED CLASS ACTION COMPLAINT**

NOTICE

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you.

**YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER OR CANNOT AFFORD ONE, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW TO FIND OUT WHERE YOU CAN GET LEGAL HELP**

Lawyer Reference Service  
Philadelphia Bar Association  
1101 Market Street, 11th Floor  
Philadelphia, PA 19107  
(215) 238-6300

AVISO

Le han demandado a usted en la corte. Si usted quiere defenderse de estas demandas expuestas en las paginas siguientes, usted tiene veinte (20) dias de plazo al partir de la fecha de la demanda y la notificacion. Hace falta asentar una comparencia escrita o en persona o con un abogado y entregar a la corte en forma escrita sus defensas o sus objeciones a las demandas en contra de su persona. Sea avisado que si usted no se defiende, la corte tomara medidas y puede continuar la demanda en contra suya sin previo aviso o notificacion. Ademas, la corte puede decidir a favor del demandante y requiere que usted cumpla con todas las provisiones de esta demanda. Usted puede perder dinero o sus propiedades y otros derechos importantes para usted.

**LLEVE ESTA DEMANDA A UN ABOGADO INMEDIATAMENTE. SI NO TIENE ABOGADO O SI NO TIENE EL DINERO SUFICIENTE DE PAGAR TAL SERVICIO. VAYA EN PERSONA O LLAME POR TELEFONO A LA OFICINA CUYA DIRECCION SE ENCUENTRA ESCRITA ABAJO PARA AVERIGUAR DONDE SE PUEDE CONSEGUIR ASISTENCIA LEGAL.**

Lawyer Reference Service  
Philadelphia Bar Association  
1101 Market Street, 11th Floor

Plaintiffs Steven Hassell and Jerome Raniell (“Plaintiffs”), individually and on behalf of the Class defined below of similarly situated persons bring this class action complaint and allege the following against Spear Wilderman, P.C. (“SW” or “Defendant”), based upon personal knowledge with respect to Plaintiffs and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

### **INTRODUCTION**

1. This is a consumer class action lawsuit brought by Plaintiffs, individually and on behalf of all others similarly situated (i.e., the Class Members), persons harmed by the data security incident (the “Data Breach”) announced by letter dated November 16, 2022 that affected clients and other individuals whose data was maintained and stored by the Defendant.

2. Defendant Spear Wilderman, P.C. is a labor law firm with locations in Philadelphia, Pennsylvania and in New Jersey.

3. On November 16, 2022, SW announced a data security incident that occurred on May 7, 2021 involving individuals’ personal identifiable information (“PII”) and personal health information (“PHI”), including the PII and PHI of the Plaintiffs. An unauthorized party infiltrated the Defendant’s network and gained access to information, potentially including the name, driver’s license or state ID number, passport number, date of birth, medical diagnosis/treatment information, financial account information and/or social security number of individuals whose information was stored by SW.

4. The Data Breach was wide-ranging, effecting thousands of individuals.

5. Despite being aware of the Data Breach for more than a year, SW did not begin mailing notice letters to those whose information was compromised until November of 2022, further compromising the individuals' PHI and PII.

6. Defendant is aware of the sensitivity of the information it maintains and is responsible to secure.

7. As a result of SW's failure to implement and follow basic security procedures, Plaintiffs' and Class Members' PII and PHI is in the hands of criminals. Plaintiffs and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiffs and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to the Defendant's failures.

8. Accordingly, Plaintiffs, individually and on behalf of all others similarly situated, allege claims for negligence and negligence *per se*, breach of fiduciary duties and confidences, violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law and injunctive/declaratory relief.

### **PROCEDURAL HISTORY**

9. Plaintiff Steven Hassell, through counsel, sent letters to SW dated December 15, 2022, January 19, 2023, and February 15, 2023 (the "Letters"), alleging that his and other potential class members (the "Class") were damaged when their personal information was allegedly subject to unauthorized access in connection with the Data Security Incident.

10. Plaintiff attached to the February 15, 2023 Letter a draft class action complaint that asserted class action claims for Negligence, Negligence *per se*, Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, et seq., Breach of Fiduciary Duty/Confidences, and Declaratory Judgment (the "Claims").

11. After considerable discussion, the Parties entered into a Tolling Agreement on March 28, 2023 as to Plaintiff Hassell's right to assert the Claims against SW, and SW's right to defend against the Claims while the Parties explore the potential for early resolution of the matter. *See* Tolling Agreement, attached hereto as **Exhibit 1**.

12. Specifically, the Tolling Agreement established that "[t]o the extent it becomes an issue in the future, the Parties agree that the Potential Plaintiff here is the first to file regarding the Data Security Incident at issue."

13. Thereafter, the parties scheduled a mediation and Plaintiff Hassell terminated the Tolling Agreement.

14. On April 14, 2023, Plaintiff Jerome Raniell filed a class action complaint in the United States District Court for the Eastern District of Pennsylvania. *See* Docket No. 2:23-cv-01442 (E.D. Pa.).

15. On April 19, 2023, Plaintiff Hassell filed his class action complaint in this Court.

### **PARTIES**

16. Plaintiff Steven Hassell is a citizen and resident of Philadelphia, Pennsylvania. Plaintiff Hassell was notified by letter dated November 16, 2022 by Defendant that his PII and PHI was compromised without authorization by an unknown third party as result of the Data Breach.

17. Plaintiff Jerome Raniell is a citizen and resident of Pittston, Pennsylvania. Plaintiff Raniell was notified by letter dated November 16, 2022 by Defendant that his PII and PHI was compromised without authorization by an unknown third party as result of the Data Breach.

18. Defendant is a labor law firm, which is located and incorporated in the Commonwealth of Pennsylvania with its principal place of business at 230 South Broad Street,

Suite 1400, Philadelphia, PA 19102 (the Philadelphia Office). See <https://spearwilder.com/> (last visited 2/8/2023).

### **JURISDICTION AND VENUE**

19. This Court has jurisdiction over this action as Plaintiffs reside in the Commonwealth of Pennsylvania. This Court also has jurisdiction over this action as Defendant continuously and systematically operates and conducts business in Philadelphia County, this Data Breach occurred in Pennsylvania and all the relevant transactions involved in this matter occurred in Pennsylvania.

20. Venue is proper in this Court pursuant to Pa. R. C. P. 1006 and 2179(a)(2) because a substantial part of events, acts, and omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this County, both Plaintiffs and Defendant reside in this County, Defendant maintains the relevant information in this County, and Defendant has caused harm to Plaintiffs and Class Members residing in this County.

### **FACTUAL BACKGROUND**

21. Defendant SW was established in 1972, when "Spear and Wilderman first formed their partnership." See <https://spearwilder.com/our-history/>. It "has devoted itself to representing both labor organizations and their members." *Id.*

22. In November of 2022, Defendant publicly disclosed "a recent data security incident that may have resulted in unauthorized access to your personal information." See Hassell Letter page 1, attached hereto as **Exhibit 2**; see Raniell Letter, attached here at **Exhibit 3**.

23. SW admitted that "[r]ecently, [it] detected and stopped a network security incident. An unauthorized third-party infiltrated our network and encrypted some of our data." *Id.* SW

disclosed that the incident occurred in May of 2021 to state Consumer Protection Bureaus. *See, e.g.,* Letter to New Hampshire Attorney General, attached hereto as **Exhibit 4**.

24. SW claims it “immediately shut off all access to the network and engaged specialized third-party forensic and technical resources to respond to the incident.” *See* Ex 2.

25. SW informed victims that the “investigation of the incident revealed that the following categories of your information may have been exposed to the unauthorized party during the compromise: name, driver’s license or state ID number, passport number, date of birth, medical diagnosis/treatment information, financial account information and/or social security number.” *Id.*

26. The victims of the Data breach include “current or former client[s] of our firm, or a party/witness to a legal matter in which our firm was involved. *Id.*

27. SW says that it “take[s] the privacy of your personal information seriously” and that “[d]ata privacy is among Spear Wilderman’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care.” *Id.*

28. SW says that it has since “secured and remediated its network and the data that we maintain,” presumably in that it claims it “reviewed and altered our tools, policies, and procedures relating to the security of our systems and servers, as well as our information life cycle management.” *Id.*

29. More than a year after the Data Breach occurred, SW mailed notification letters to all affected individuals informing them about the Data Breach. In these letters, Defendants offered affected individuals the opportunity to enroll in free credit monitoring and identity restoration services through a product provided by “Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.” *Id.*

30. The notification letters were untimely and deficient as a matter of law, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive information was stored on systems without adequate security, the deficiencies in the security systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether SW knows if the data has not been further disseminated. *Id.*

31. Further, SW's efforts to protect those affected were limited to the letter. SW has a number of ways to communicate with individuals whose information it maintains, yet SW took no steps to do so other than through the one notice letter. Upon information and belief, Defendant did not post notices in union locations, provide training or information to union leaders, run programs for current clients or related individuals and/or its own employees.

32. SW admitted that “[a]n unauthorized third-party infiltrated our network and encrypted some of our data” but claimed that it “found no evidence that your information has been specifically misused as a result of the compromise” and that:

**As of this writing, Spear Wilderman has not received any reports of related identity theft since the date of the incident.**

*Id.* SW failed to take steps necessary to inform Plaintiffs and Class Members that their data was in fact exposed to third party bad actors.

33. SW obtains, collects, and stores a massive amount of data. It says that it “values the privacy and importance of your personal data” and acknowledges that it is responsible to safeguard Plaintiffs and Class Members’ PII and PHI. It pledges that it takes privacy very seriously and promises that it will maintain the security and privacy of information in its possession. Yet it has failed, and continues to fail, to take data security seriously.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII and PHI, SW assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs and Class Members' information from disclosure.

35. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI and they rely on SW to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

**SW Knew the Risks of Storing Valuable PII and PHI  
and the Foreseeable Harm to Victims**

36. SW understands the PII and PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes and that, as a result, SW's systems would be attractive targets for cybercriminals.

37. SW also knew that any breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose PII and PHI was compromised, as well as intrusion into their highly private health information.

38. These risks are not merely theoretical; in recent years, numerous high-profile breaches have occurred at businesses such as Equifax, Yahoo, Marriott, Anthem, and many others.

39. PII has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."<sup>1</sup> PHI, in addition to being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

---

<sup>1</sup> Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/>.



40. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.”

41. Even if stolen PII or PHI does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

#### **Plaintiffs and Class Members Suffered Damages**

42. For the reasons mentioned above, SW’s conduct, which allowed the Data Breach to occur, caused Plaintiffs and members of the Class significant injuries and harm in several ways. Plaintiffs and members of the Class must immediately devote time, energy, and money to:

- 1) closely monitor their medical statements, bills, records, and credit and financial accounts;
- 2) change login and password information on any sensitive account even more frequently than they already do;
- 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and
- 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

43. For example, Plaintiffs have already suffered and will continue to suffer lost personal time spent reviewing their credit reports and checking their medical billing and statements from their health insurer and/or providers, as they were specifically directed to do by SW as a result of the Data Breach. *See* Ex. 2.

44. Once PII or PHI is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of SW's conduct. Further, the value of Plaintiffs' and Class members' PII and PHI has been diminished by its exposure in the Data Breach.

45. As a result of SW's failures, Plaintiffs and Class members are at substantial increased risk of suffering identity theft and fraud or misuse of their PII and PHI.

46. The reality is that cybercriminals seek nefarious outcomes from a data breach" and "stolen health data can be used to carry out a variety of crimes."<sup>2</sup>

47. Plaintiffs and the Class members have also been injured by SW's unauthorized disclosure of their records.

48. Plaintiffs and Class members are at a continued risk because their information remains in SW's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as SW fails to undertake the necessary and appropriate security and training measures to protect PII and PHI.

49. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.<sup>3</sup> Indeed, a robust

---

<sup>2</sup> <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon>.

<sup>3</sup> Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft>.

“cyber black market” exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

50. The ramifications of Defendant’s failure to keep PII and PHI secure are long lasting and severe. Once 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.

51. Further, criminals often trade stolen PHI and PII on the “cyber black-market” for years following a breach. Cybercriminals can post stolen PHI and PII on the internet, thereby making such information publicly available.

52. The Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.<sup>4</sup> This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim’s ability to detect and address the harm.

53. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual’s employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual’s authentic tax return is rejected.

54. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and

---

<sup>4</sup> *Identity Theft and Your Social Security Number*, Social Security Administrative, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

55. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”<sup>5</sup>

56. Defendant knew, or should have known, the importance of safeguarding PHI and PII entrusted to it and of the foreseeable consequences if its systems were breached. This includes the significant costs that would be imposed on individuals as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

57. Plaintiffs and Class Members now face years of constant surveillance of their records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PHI and PII.

58. Despite all of the publicly available knowledge of the continued compromises of PHI and PII, SW’s approach to maintaining the privacy of the PHI and PII was in the very least, negligent.

59. In all contexts, time has constantly been recognized as compensable, and for many people, it is the basis on which they are compensated. Plaintiffs and Class Members should be spared having to deal with the consequences of Defendant’s misfeasance.

---

<sup>5</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft>.

60. Once PHI and PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.<sup>6</sup>

61. SW's delay in identifying and reporting the Data Breach caused additional harm to Plaintiffs and Class Members. Plaintiffs were not timely notified of the Data Breach, depriving them and the Class of the ability to promptly mitigate potential adverse resulting consequences.

62. As a result of SW's failure to prevent the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;
- b. Unauthorized use and misuse of their PHI and PII;
- c. The loss of the opportunity to control how their PHI and PII is used;
- d. The diminution in value of their PHI and PII;
- e. The compromise, publication, and/or theft of their PHI and PII;
- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- g. Lost opportunity costs and lost wages associated with effort 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;
- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;
- j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PHI and PII being placed in the hands of

---

<sup>6</sup> 2014 LexisNexis True Cost of Fraud Study, available at <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>.

criminals;

- k. The continued risk to their PHI and PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PHI and PII in its possession; and
- l. 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 Plaintiffs and Class Members.

63. To date, SW has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures it has taken to secure the PII and PHI still in its possession. Through this litigation, Plaintiffs seek to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure SW has proper measures in place to prevent another breach from occurring in the future.

64. SW was expressly prohibited by the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

65. 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.<sup>7</sup>

66. In 2016, the FTC updated its publication, *Protecting Personal Information: A*

---

<sup>7</sup> Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

*Guide for Business*, which established cybersecurity guidelines for businesses.<sup>8</sup> 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.

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect 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 FTCA, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. SW failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against unauthorized access to PHI and PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

69. SW was at all times fully aware of its obligation to protect PHI and PII and was also aware of the significant repercussions that would result from its failure to do so.

**As a Law Firm, Defendant should have known it was at risk of Cyberattack**

70. Law firms are particularly susceptible to cyberattack. It is well known in the industry that data protection is important for law firms.<sup>9</sup>

---

<sup>8</sup> Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

<sup>9</sup> See <https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/> (last visited 2/9/23); see also <https://www.attorneyatwork.com/25-percent-of-law-firms-breached-cybersecurity-trends/> (last visited 2/9/2023).

71. In fact, a number of firms have been hit with cyberattacks, which have been well publicized in the industry.<sup>10</sup>

72. Law firms have always been on notice of the inherent risk of a data breach and their obvious duty to maintain the confidentiality of records they maintain.<sup>11</sup> This concern has been made more apparent and obvious in light of the increase in remote work since 2020.<sup>12</sup>

73. As such, SW had a duty to maintain and secure the PHI and PII that was exposed and failed to do so to the detriment of the Plaintiffs and the Class.

### **CLASS ACTION ALLEGATIONS**

74. Plaintiffs bring this class action pursuant to Rules 1701-1706 of the Pennsylvania Rules of Civil Procedure on behalf of themselves and all others similarly situated. The Class that Plaintiffs seek to represent is defined as follows:

**All persons whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Data Breach on or around November 16, 2022 (The “Class”).**

75. Excluded from the Class are: (i) Defendant and its officers, directors, affiliates, and subsidiaries (ii) the Judge presiding over this action and the court staff in this case and (iii) any

---

<sup>10</sup> See <https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks/> (last visited 2/9/23); see also <https://www.law.com/americanlawyer/2023/01/05/november-cyberattack-hobbled-cadwalader-for-weeks-internal-emails-show/> (last visited 2/9/23).

<sup>11</sup> See ABA Model Rule 1.6(c) (requiring “reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information”); ABA Model Rule 1.1, (requiring that lawyers stay abreast of changes in technology); ABA Model Rules 5.1 and 5.3 (requiring that lawyers properly supervise other lawyers and third-party electronic information storage vendors). See also Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (securing communication of protected client information) (May 2017); Comm. on Ethics & Prof’l Responsibility, Formal Op. 483 (Lawyers’ Obligations After an Electronic Data Breach or Cyberattack) (October 2018).

<sup>12</sup> See, e.g., Comm. on Ethics & Prof’l Responsibility, Formal Op. 498 (Virtual Practice) (March 2021).



other person or entity found by a court of competent jurisdiction to be guilty of initiating, causing, aiding or abetting the criminal activity occurrence of the Data Breaches or who pleads *nolo contendere* to any such charge.

76. Plaintiffs reserve the right to modify or amend the definition of the proposed Class as additional information becomes available to Plaintiffs.

77. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

78. **Numerosity**: The members of the Class are so numerous that joinder of all members of the Class is impracticable. Plaintiffs are informed and believe that the proposed Class includes individuals who have been damaged by Defendant's conduct as alleged herein. The precise number of Class members is unknown to Plaintiffs but can be ascertained from Defendant's records.

79. **Commonality**: This action involves common questions of law and fact, which predominate over any questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- a. whether Defendant engaged in the wrongful conduct alleged herein;
- b. whether the alleged conduct constitutes violations of the laws asserted;
- c. whether Defendant owed Plaintiffs and the other Class members a duty to adequately protect their PII/PHI;
- d. whether Defendant breached its duty to protect the PII/PHI of Plaintiffs and the other Class members;
- e. whether Defendant knew or should have known about the inadequacies of its data protection, storage, and physical property security;
- f. whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiffs' and the other Class

members' PII/PHI from unauthorized theft, release, or disclosure;

- g. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendant's offices and computer systems to safeguard and protect Plaintiffs' and the other Class members' PII/PHI from unauthorized theft, release or disclosure;
- h. whether Defendant breached its promise to keep Plaintiffs' and the Class members' PII/PHI safe and to follow data security protocols;
- i. whether Defendant's conduct was the proximate cause of Plaintiffs' and the other Class members' injuries;
- j. whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;
- k. whether Plaintiffs and the other Class members suffered ascertainable and cognizable injuries as a result of Defendant's conduct;
- l. whether Plaintiffs and the other Class members are entitled to recover actual damages; and
- m. whether Plaintiffs and the other Class members are entitled to other appropriate remedies, including injunctive relief.

80. Defendant engaged in a common course of conduct giving rise to the claims asserted by Plaintiffs on behalf of herself and the other Class members. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

81. **Typicality**: Plaintiffs' claims are typical of the claims of the members of the Class. All Class members were subject to the Data Breach and had their PII/PHI accessed by and/or disclosed to unauthorized third parties. Defendant's misconduct impacted all Class members in the same manner and arose from the same set of operative facts and are based on the same set of legal theories.

82. **Adequacy of Representation**: Plaintiffs will fairly and adequately protect the interests of the members of the Class, have retained counsel experienced in complex consumer

class action litigation and intends to prosecute this action vigorously. Plaintiffs have no adverse or antagonistic interests to those of the Class.

83. **Superiority**: A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Defendant. It would thus be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

**FIRST CAUSE OF ACTION**  
**Negligence and Negligence *per se***  
**(On Behalf of Plaintiffs and the Class)**

84. Plaintiffs re-allege the paragraphs above as if fully set forth herein.

85. Defendant had a duty to exercise reasonable care to protect and secure Plaintiffs' and the Class Members' PII/PHI.

86. Through its acts and omissions, Defendant violated its duty to use reasonable care to protect and secure Plaintiffs' and Class Members' PII/PHI.

87. Defendant breached the duties owed to Plaintiffs and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of information that resulted in the unauthorized access and compromise of PII/PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and

implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices.

88. It was reasonably foreseeable that Defendant's failure to exercise reasonable care to protect and secure Plaintiffs' and Class Members' PII/PHI would result in an unauthorized third-party gaining access to, possession of, and control over such information for an unlawful purpose.

89. Defendant breached its duty to Plaintiffs and the Class members by failing to implement and maintain security controls that were capable of adequately protecting the PII/PHI entrusted to it.

90. Defendant's failure to adequately protect Plaintiffs' and Class Members' PII/PHI was negligent.

91. Plaintiffs' and Class Members' PII/PHI constitute personal property and due to Defendant's negligence their PII/PHI was exposed or stolen, resulting in harm to Plaintiffs and Class Members.

92. Section 5 of the FTC Act prohibits unfair or deceptive practices that affect commerce, including those business practices Defendant engaged in and its failure to protect Plaintiffs' and Class members' PII/PHI. *See* 15 U.S.C. § 45. Given Defendant's acute awareness of the sensitivity and privacy concerns surrounding the PII/PHI of Plaintiffs and Class members, Defendant was on notice of the likely consequences from such a breach and the impact it would have on Plaintiffs and Class members.

93. Defendant's negligence in failing to exercise reasonable care in protecting the PII/PHI of Plaintiffs and the other Class members is further evinced by Defendant's failure to comply with legal obligations and industry standards, and the significant delay between the date of the Data Breach and the time when the Data Breach was disclosed.

94. The injuries to Plaintiffs and the other Class members were reasonably foreseeable to Defendant because laws and statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the Class members' PII/PHI.

95. The injuries to Plaintiffs and the other Class members also were reasonably foreseeable because Defendant knew or should have known that systems used for safeguarding PII/PHI were inadequately secured and exposed PII/PHI to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Defendant's own misconduct created a foreseeable risk of harm to Plaintiffs and the other Class members.

96. Defendant's failure to take reasonable steps to protect the PII/PHI of Plaintiffs and the members of the Class was a proximate cause of their injuries because it directly allowed thieves easy access to Plaintiffs' and the Class members' PII/PHI. This ease of access allowed thieves to steal PII/PHI of Plaintiffs and the other members of the Class, which could lead to dissemination in black markets.

97. As a direct and proximate result of Defendant's conduct, Plaintiffs and the Class members have suffered theft of their PII/PHI. Defendant allowed thieves access to Class members' PII/PHI, thereby decreasing the security of Class members' financial and health accounts, making Class members' identities less secure and reliable, and subjecting Class members to the imminent threat of identity theft. Not only will Plaintiffs and the members of the Class have to incur time

and money to re-secure their bank accounts/health insurance accounts, medical records, and identities, but they will also have to protect against identity theft for years to come.

98. Additionally, Plaintiffs and Class members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the benefit of their bargain with Defendant; (ii) the publication and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity 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 tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII/PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives.

99. Defendant actively offered services to or maintained the records of Plaintiffs and the Class, wherein it used, handled, processed, and stored the PII/PHI of Plaintiffs and the Class members without disclosing that its security was inadequate and unable to protect their PII/PHI. Holding Defendant accountable for its negligence will further the policies embodied in such law by incentivizing businesses like law firms to properly secure sensitive information and protect people who rely on these companies.

**SECOND CAUSE OF ACTION**  
**PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION**  
**LAW, 73 P.S. §§ 201-1, et seq.**  
**(On Behalf of the Plaintiffs and the Class)**

100. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

101. SW is a “person,” as meant by 73 P.S. § 201-2(2).

102. Plaintiffs and Class Members purchased goods and/or services from SW primarily for personal, family and/or household purposes.

103. SW engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 P.S. § 201-3, including the following:

- a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));
- b. Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201-2(4)(vii));
- c. Failing to comply with the terms of any written guarantee or warranty given to the buyer at, prior to or after a contract for the purchase of goods or services is made (73 P.S. § 201-2(4)(xiv)); and
- d. Engaging in any other fraudulent or deceptive conduct which creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

104. Defendant’s unfair or deceptive acts and practices include:

- e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ and Class Members’ PII and PHI, which was a direct and proximate cause of the Data Breach;
- f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures in response to increasing cybersecurity risks in the legal sector, which was a direct and proximate cause of the Data Breach;
- g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs’ and Class Members’ PII and PHI,

including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505, as well as its own policies, which was a direct and proximate cause of the Data Breach;

- h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII and PHI, including by implementing and maintaining reasonable security measures;
- i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI;
- j. Failing to timely and adequately notify Plaintiffs and Class Members of the Data Breach;
- k. Misrepresenting that certain sensitive PII and PHI was not accessed during the Data Breach, when it was;
- l. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' PII and PHI; and
- m. Omitting, suppressing, and concealing the material fact that it did not comply with the common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII and PHI, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15 U.S.C. §§ 6501–6505 and Lawyer rules.

105. SW's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Class Members, about the adequacy of its data security and ability to protect the confidentiality of PII and PHI.

106. SW's representations and omissions were material because they were likely to deceive reasonable individuals, including Plaintiffs and the Class Members, leading them to believe for several months that their PII and PHI was secure and that they did not need to take actions to secure their identities.

107. SW intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.



108. Had SW disclosed to Plaintiffs and Class Members that its network systems were not secure and thus vulnerable to attack it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Plaintiffs and Class Members entrusted SW with their sensitive and valuable PII and PHI. SW accepted the responsibility of being a steward of this data, while failing to disclose the inadequacy of its security measures . Accordingly, because SW held itself out as maintaining a secure system for PII and PHI data, Plaintiffs and Class Members acted reasonably in relying on its misrepresentations and omissions, the truth of which they could not have discovered.

109. SW acted intentionally, knowingly, willfully, wantonly, maliciously, and outrageously to violate Pennsylvania's Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiffs' and Class Members' rights.

110. As a direct and proximate result of SW's unfair methods of competition and unfair or deceptive acts or practices and Plaintiffs' and Class Members' reliance on them, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring financial accounts for fraudulent activity; imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

111. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$100 (whichever is greater), treble damages, punitive damages, attorneys' fees or costs, and any additional relief the Court deems necessary or proper.

**THIRD CAUSE OF ACTION**  
**BREACH OF FIDUCIARY DUTY/CONFIDENCES**  
**(On Behalf of Plaintiffs and the Class)**

112. Plaintiffs restate and reallege all proceeding allegations above as if fully set forth herein.

113. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII and PHI about them that was conveyed to, collected by, and maintained by SW and that was ultimately accessed or compromised in the Data Breach.

114. As a law firm, SW has a fiduciary relationship to the people who participate in a legal case involving their clients, including Plaintiffs and the Class members.

115. Because of that fiduciary and special relationship, SW was provided with and stored private and valuable information related to Plaintiffs and the Class which it was required to maintain in confidence.

116. SW owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

117. As a result of the parties' relationship, SW had an obligation to maintain the confidentiality of the information.

118. Clients like Plaintiffs and Class members have a privacy interest in personal matters, which SW had a fiduciary duty not to disclose.

119. As a result of the parties' relationship, SW had possession and knowledge of confidential records of Plaintiffs and Class members, information not generally known.

120. Plaintiffs and Class members did not consent to nor authorize SW to release or disclose their information to an unknown criminal actor.

121. SW breached the duties owed to Plaintiffs and Class Members and thus was negligent. SW breached these duties by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII and PHI; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' information to a criminal third party.

122. But for SW's wrongful breach of its duties and confidences owed to Plaintiffs and Class Members, their privacy, confidences, PII, and PHI would not have been compromised.

123. As a direct and proximate result of SW's breach of its fiduciary duty, Plaintiffs and Class Members have suffered injuries, including:

- a. Theft of their PII and/or PHI;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;
- c. Costs associated with purchasing credit monitoring and identity theft protection services;
- d. Lowered credit scores resulting from credit inquiries following fraudulent activities;
- e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the SW Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing

accounts, and imposing withdrawal and purchase limits on compromised accounts;

- f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII and/or PHI being placed in the hands of criminals;
- g. Damages to and diminution in value of their PII and PHI entrusted, directly or indirectly, to SW with the mutual understanding that SW would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;
- h. Continued risk of exposure to hackers and thieves of their PII and/or PHI, which remains in SW's possession and is subject to further breaches so long as SW fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;
- i. Loss of their privacy and confidentiality in their PHI;
- j. The erosion of the essential and confidential relationship between SW – as a law firm – and Plaintiffs and Class members as participants in lawsuits; and
- k. Loss of personal time spent carefully reviewing statements to check for charges for services not received, as directed to do by SW.

124. Additionally, SW received direct and indirect payments from or on behalf of Plaintiffs and Class members for services with the understanding that SW would uphold its fiduciary responsibilities to maintain the confidences of Plaintiffs and Class members' private information.

125. SW breached the confidence of Plaintiffs and Class members when it made an unauthorized release and disclosure of their confidential information and/or PHI.

126. It would be inequitable for SW to retain the benefit at Plaintiffs and Class members' expense.

127. As a direct and proximate result of SW's breach of its fiduciary duty, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

**FIFTH CAUSE OF ACTION**  
**DECLARATORY JUDGMENT**  
**(On Behalf of Plaintiffs and the Class)**

128. Plaintiffs and the Class restate and reallege all proceeding allegations above as if fully set forth herein.

129. This cause of action is brought under 28 U.S.C. § 2201. This Court is authorized to declare rights, status, and other legal relations, and such declarations shall have the force and effect of a final judgment or decree. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious as described in this Complaint.

130. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and Class Members' PII/PHI and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII/PHI. Plaintiffs allege that Defendant's data security measures remain inadequate, contrary to its assertion that it has confirmed the security of its network and its systems.

131. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of PII/PHI and remain at imminent risk that further compromises will occur in the future.

132. This Court should enter a judgment declaring, among other things, the following:
- a. Defendant owes a legal duty to secure PII/PHI and to timely notify those affected of the Data Breach; and
  - b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII/PHI.

133. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect PII/PHI.

134. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach at SW occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

135. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to SW if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to SW of complying with an injunction by employing reasonable prospective data security measures and communicating those measures to the Class is relatively minimal, and it has a pre-existing legal obligation to employ such measures.

136. 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 SW, thus eliminating the additional injuries that would result to Plaintiffs and to those whose PII would be further compromised.

137. Plaintiffs and the Class, therefore, seek a declaration (1) that SW's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their obligations and duties of care, SW must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

- d. Ordering that Defendant segment PII/PHI data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner all data not necessary for its provisions of services;
- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct 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
- h. Ordering Defendant to meaningfully educate employees and members about the threats they face as a result of the loss of their PII/PHI to third parties, as well as the steps they must take to protect themselves.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, on behalf of himself and all other similarly situated, prays for relief as follows:


- a. For an order certifying the Class and naming Plaintiffs as representative of the Class and Plaintiffs' attorneys as Class Counsel to represent the Class;
- b. For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;
- c. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;
- d. For an order of restitution and all other forms of equitable monetary relief;
- e. Declaratory and injunctive relief as described herein;
- f. Awarding Plaintiffs' reasonable attorneys' fees, costs, and expenses;
- g. Awarding pre- and post-judgment interest on any amounts awarded; and
- h. Awarding such other and further relief as may be just and proper.

**JURY TRIAL DEMANDED**

Plaintiffs, on behalf of themselves and the Class, demand a trial by jury on all issues so triable.

Dated: September 22, 2023

Respectfully submitted,

  
\_\_\_\_\_  
/s/ Kevin W. Fay, Esq.  
PA Bar No. 308252  
**GOLOMB SPIRT, P.C.**  
1835 Market Street, Suite 2900  
Philadelphia, PA 19103  
Telephone: (215) 985-9177  
[kfay@golomblegal.com](mailto:kfay@golomblegal.com)

*/s/ Charles E. Schaffer*  
\_\_\_\_\_  
Charles E. Schaffer (PA BAR # 76259)  
Nicholas J. Elia (PA BAR # 325978)  
**LEVIN SEDRAN & BERMAN**  
510 Walnut St., Ste. 500  
Philadelphia, PA 19106  
Phone: (215) 592-1500  
[cschaffer@lfsblaw.com](mailto:cschaffer@lfsblaw.com)  
[nelia@lfsblaw.com](mailto:nelia@lfsblaw.com)

**THE LYON LAW FIRM, LLC**  
Joseph M. Lyon\*  
2754 Erie Ave.  
Cincinnati, OH 45208  
Phone: (513) 381-2333  
Fax: (513) 766-9011  
[jlyon@thelyonfirm.com](mailto:jlyon@thelyonfirm.com)

*Attorneys for Plaintiffs and the Class*



# EXHIBIT 1

## TOLLING AGREEMENT

This Tolling Agreement (“Agreement”) is effective as of March 28, 2023 (“Effective Date”), by Spear Wilderman, P.C. (“SW”), on the one hand, and Steven Hassell (“Potential Plaintiff”), on the other hand (each referred to individually as a “Party” and collectively as the “Parties”), to be executed on behalf of the Parties’ counsel.

### Recitals

WHEREAS, on or about November 16, 2022, the Potential Plaintiff received notice from SW of a data security incident that may have resulted in unauthorized access to personal information (the “Data Security Incident”);

WHEREAS, the Potential Plaintiff, through counsel, sent letters to SW dated December 15, 2022, January 19, 2023, and February 15, 2023 (the “Letters”), alleging that his and other potential class members (the “Class”) were damaged when their personal information was allegedly subject to unauthorized access in connection with the Data Security Incident;

WHEREAS, the Potential Plaintiff attached to the February 15, 2023 Letter a draft class action complaint that asserted class action claims for Negligence, Negligence *per se*, Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-1, *et seq.*, Breach of Fiduciary Duty/Confidences, and Declaratory Judgment (the “Claims”);

WHEREAS, the Parties have agreed to enter into a tolling agreement as to Potential Plaintiff’s rights to assert the Claims against SW, and SW’s right to defend against the Claims while the Parties explore the potential for early resolution of the matter.

NOW, THEREFORE, in consideration of the mutual promises and agreements contained herein, the sufficiency of which is hereby acknowledged, the Parties agree as follows:

### Terms and Conditions

1. **Tolling of Statute of Limitations.** The Parties agree that any applicable statutes of limitations, statutes of repose, doctrines of laches, or any other time-based limitation, bar, or defense that may pertain or apply to the Claims between the Parties (collectively, the “Time-Related Defenses”) shall be tolled for a period beginning on the Effective Date and ending on the Termination Date of this Agreement (the “Tolling Period”). The Tolling Period shall be excluded from and not be counted in computing the running of time for the purpose of any Time-Related Defenses. The Tolling Period shall not waive or preclude any statutes of limitations, statutes of repose, doctrines of laches, or any other time-based limitation, bar or defense under any applicable law that may pertain or apply to a lawsuit

filed by the Potential Plaintiff which would have barred the Claims prior to the Effective Date.

**2. Tolling Period; Termination.** This Agreement and the Tolling Period shall terminate on the first business day following the earlier of: (a) sixty (60) calendar days from the Effective Date; or (b) seven (7) calendar days following the receipt by any Party of written notice terminating this Agreement (the “Termination Date”). The termination of this Agreement by one Party shall operate to terminate this Agreement as to all Parties. The Termination Date may be extended for an additional period if the Parties agree in writing.

**3. No Alteration of Limitations Periods.** Nothing contained in this Agreement shall be deemed to shorten any statute of limitations nor shall anything in this agreement be deemed to revive any statute of limitations that has lapsed as of the Effective Date.

**4. Forbearance from the Initiation of Suit; Investigation of Claims.** No Party shall initiate any legal proceeding or other Claims against the other during the Tolling Period. At the same time, nothing in this Agreement shall preclude any Party from investigating the Claims, or any defenses to such Claims, nor shall any such investigation constitute a breach of this Agreement.

**5. Acknowledgement of Claim.** To the extent it becomes an issue in the future, the Parties agree that the Potential Plaintiff here is the first to file regarding the Data Security Incident at issue.

**6. Notices.** Any notices provided under this Agreement shall be given in writing, by certified mail, return receipt requested, and by e-mail, addressed as follows:

**If to the Potential Plaintiff:**

Kenneth J. Grunfeld  
Golomb Spirt Grunfeld, P.C.  
1835 Market Street, Suite 2900  
Philadelphia, PA 19103  
[kgrunfeld@golomblegal.com](mailto:kgrunfeld@golomblegal.com)

**If to SW:**

Edward J. McAndrew  
Baker & Hostetler LLP  
1735 Market Street, Suite 3300  
Philadelphia, PA 19103-7501  
[emcandrew@bakerlaw.com](mailto:emcandrew@bakerlaw.com)

**7. No Admissions.** This Agreement shall not be deemed an admission of any kind by any Party. Except as expressly stated herein, the Parties expressly reserve and do not waive any and all rights, claims, causes of action, arguments, and defenses that they may have.

8. **Inadmissibility.** This Agreement is not admissible before a jury in any subsequent action arising from the Data Security Incident or the Claims, although the Court may give an appropriate instruction about the limitations period.

9. **Choice of Law.** This Agreement constitutes the entire understanding and agreement between the Parties as to its subject matter and supersedes any other agreements related to the subject matter hereof. This Agreement may be modified only by a written agreement signed by the Parties. This Agreement shall be governed by and construed according to Pennsylvania law.

10. **Authorization.** Counsel executing this Agreement on behalf of each Party warrants and represents that he or she has been duly authorized by that Party to execute this Agreement on behalf of that Party.

11. **Counterparts.** This Agreement may be executed in two or more counterparts, each of which shall be deemed an original as against any party whose signature appears thereon, and all of which, when taken together, shall constitute one and the same instrument.

**IN WITNESS WHEREOF**, the Parties have caused this Agreement to be executed by their duly authorized representatives as of the dates written below.

**Kenneth J. Grunfeld,  
For Potential Plaintiff**

**Edward J. McAndrew,  
For Spear Wilderman, P.C.**



\_\_\_\_\_  
Signature

\_\_\_\_\_  
Signature

Name: Kenneth J. Grunfeld

Name: Edward J. McAndrew

Title: Partner

Title: Partner

Date: March 28, 2023

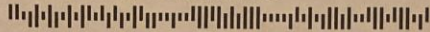
Date: March 28, 2023

# EXHIBIT 2

Spear Wilderman, P.C.  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998

SPEAR WILDERMAN, P.C.

PHOEJQ00202486  
STEVEN HASSELL  
5901 N HUTCHINSON ST 1  
PHILADELPHIA, PA 19141-3713



November 16, 2022

Notice of Data Security Incident

Dear Steven Hassell,

We are writing in order to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. At this time, we are unaware of any fraudulent misuse of your personal information. However, we take the privacy of your personal information seriously, and want to provide you with information and resources you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

Recently, Spear Wilderman, P.C. ("Spear Wilderman") detected and stopped a network security incident. An unauthorized third-party infiltrated our network and encrypted some of our data. We immediately shut off all access to the network and engaged specialized third-party forensic and technical resources to respond to the incident. Spear Wilderman has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the cause and extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused as a result of the compromise, an investigation of the incident revealed that the following categories of your information may have been exposed to the unauthorized party during the compromise: name, driver's license or state ID number, passport number, date of birth, medical diagnosis/treatment information, financial account information and/or social security number. This information was maintained because you were a current or former client of our firm, or a party/witness to a legal matter in which our firm was involved. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

**As of this writing, Spear Wilderman has not received any reports of related identity theft since the date of the incident.**

What We Are Doing:

Data privacy is among Spear Wilderman's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, we moved quickly to initiate our incident response, which included fully securing and remediating our network and the data that we maintain. We conducted an investigation with the assistance of third-party forensic specialists, and have reported this matter to law enforcement. We have reviewed and altered our tools, policies, and procedures relating to the security of our systems and servers, as well as our information life cycle management.

REG

Case ID: 230401942

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

We encourage you to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/spearwilderman> and follow the instructions provided. When prompted please provide the following unique code to receive services: **VXBPPXWVAL**. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Again, at this time, there is no evidence that your information has been taken or misused. However, we encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-877-511-0010 and supply the fraud specialist with your unique code listed above.

Spear Wilderman values the privacy and importance of your personal data, and we apologize for any inconvenience or concern that this incident has caused.

Sincerely,

*Denise H. Miller*

Denise H. Miller  
Administrator, Spear Wilderman, P.C.

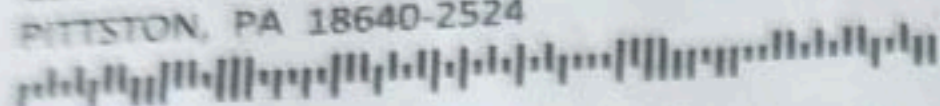
# EXHIBIT 3



SPEAR WILDERMAN, P.C.

Spear Wilderman, P.C.  
c/o CyberScout  
PO Box 1286  
Dearborn, MI 48120-9998

PH0EJQ00210712  
JERRY RANIELL  
196 MARKET ST  
PITTSBURGH, PA 15222-2524



November 16, 2022

Notice of Data Security Incident

PH0EJQ0021071210712010280400

Dear Jerry Raniell,

We are writing in order to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. At this time, we are unaware of any fraudulent misuse of your personal information. However, we take the privacy of your personal information seriously, and want to provide you with information and resources you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

Recently, Spear Wilderman, P.C. ("Spear Wilderman") detected and stopped a network security incident. An unauthorized third-party infiltrated our network and encrypted some of our data. We immediately shut off all access to the network and engaged specialized third-party forensic and technical resources to respond to the incident. Spear Wilderman has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the cause and extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused as a result of the compromise, an investigation of the incident revealed that the following categories of your information may have been exposed to the unauthorized party during the compromise: name, driver's license or state ID number, passport number, date of birth, medical diagnosis/treatment information, financial account information and/or social security number. This information was maintained because you were a current or former client of our firm, or a party/witness to a legal matter in which our firm was involved. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

**As of this writing, Spear Wilderman has not received any reports of related identity theft since the date of the incident.**

What We Are Doing:

Data privacy is among Spear Wilderman's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, we moved quickly to initiate our incident response, which included fully securing and remediating our network and the data that we maintain. We conducted an investigation with the assistance of third-party forensic specialists, and have reported this matter to law enforcement. We have reviewed and altered our tools, policies, and procedures relating to the security of our systems and servers, as well as our information life cycle management.

### Steps You Can Take to Help Protect Your Information

**Credit Reports:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

**Experian**  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

**Equifax**  
P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

**Experian**  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

**File Police Report:** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**FTC and Attorneys General:** You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

---

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**For residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf) or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For residents of Oregon:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission** - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General** Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General** Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General** - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General** - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General** - Consumer Protection Division: 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General** - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General** - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General** - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)

# EXHIBIT 4

November 17, 2022

**Ryan M. Cook**  
601.499.8087 (direct)  
601.499.8077 (main)  
Ryan.Cook@WilsonElser.com

Via electronic-mail: [DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov); [AttorneyGeneral@doj.nh.gov](mailto:AttorneyGeneral@doj.nh.gov)

**Attorney General John Formella**  
Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03302

**Re: Our Client : Spear Wilderman, P.C.**  
**Matter : Data Security Incident on May 7, 2021**  
**Wilson Elser File # : 16516.0504**

---

Dear Attorney General Formella:

We represent Spear Wilderman, P.C. (“SWP”), a labor law firm with locations in Pennsylvania and New Jersey, with respect to a potential data security incident described in more detail below. SWP takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that SWP is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

On May 7, 2021, SWP detected and stopped a cybersecurity attack against its network. This incident may have resulted in the exposure of personal information. Although we have found no evidence that any information has been specifically accessed for misuse, it is possible that the potentially impacted name, driver’s license or state ID number, passport number, date of birth, medical diagnosis/treatment information, financial account information and/or social security number could have been exposed as a result of this attack.

As of this writing, SWP has not received any reports of related identity theft since the date of the incident (May 7, 2021 to present).

2. Number of New Hampshire Residents Affected

A total of thirty (30) New Hampshire residents were potentially affected by this security incident. Notification letters to all potentially impacted individual were mailed on November 16, 2022, by first class mail. A sample copy of the notification letter is included with this letter.

3. Steps Taken

Immediately upon learning of this incident, SWP contacted a reputable third-party forensic team to assist with its investigation. Since then, SWP has been working with cyber experts to help respond to this incident and review all policies and procedures relating to the security of SWP's systems.

Although SWP is not aware of any evidence of misuse of personal information, SWP extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through Cyberscout. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

4. Contact Information

SWP remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Ryan.Cook@WilsonElser.com or 601-499-8087.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**

Ryan Cook, Esq.

Copy: Robert Walker, Esq.  
(Wilson Elser LLP)

Enclosure: *Sample Notification Letter*



November 16, 2022

Notice of Data Security Incident

Dear [REDACTED],

We are writing in order to inform you of a recent data security incident that may have resulted in unauthorized access to your personal information. At this time, we are unaware of any fraudulent misuse of your personal information. However, we take the privacy of your personal information seriously, and want to provide you with information and resources you can use to protect your information. This letter contains information about the incident and information about how to protect your personal information going forward.

What Happened and What Information was Involved:

Recently, Spear Wilderman, P.C. (“Spear Wilderman”) detected and stopped a network security incident. An unauthorized third-party infiltrated our network and encrypted some of our data. We immediately shut off all access to the network and engaged specialized third-party forensic and technical resources to respond to the incident. Spear Wilderman has secured and remediated its network and the data that we maintain.

Once our environment was secure, we immediately initiated a comprehensive investigation into the cause and extent of the unauthorized activity. Although we have found no evidence that your information has been specifically misused as a result of the compromise, an investigation of the incident revealed that the following categories of your information may have been exposed to the unauthorized party during the compromise: name, driver’s license or state ID number, passport number, date of birth, medical diagnosis/treatment information, financial account information and/or social security number. This information was maintained because you were a current or former client of our firm, or a party/witness to a legal matter in which our firm was involved. Notably, the types of information affected varied by individual, and not every individual had every element exposed.

**As of this writing, Spear Wilderman has not received any reports of related identity theft since the date of the incident.**

What We Are Doing:

Data privacy is among Spear Wilderman’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon detecting this incident, we moved quickly to initiate our incident response, which included fully securing and remediating our network and the data that we maintain. We conducted an investigation with the assistance of third-party forensic specialists, and have reported this matter to law enforcement. We have reviewed and altered our tools, policies, and procedures relating to the security of our systems and servers, as well as our information life cycle management.

Case ID: 230401942

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do:

We encourage you to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

To enroll in Credit Monitoring services at no charge, please log on to <https://secure.identityforce.com/benefit/spearwilderman> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Again, at this time, there is no evidence that your information has been taken or misused. However, we encourage you to take full advantage of this service offering. Cyberscout representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line 1-877-511-0010 and supply the fraud specialist with your unique code listed above.

Spear Wilderman values the privacy and importance of your personal data, and we apologize for any inconvenience or concern that this incident has caused.

Sincerely,

Denise H. Miller  
Administrator, Spear Wilderman, P.C.



## Steps You Can Take to Help Protect Your Information

**Credit Reports:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

[www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

### **Equifax**

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

### **Experian**

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

### **TransUnion**

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

### **Equifax**

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

**File Police Report:** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

**FTC and Attorneys General:** You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

Case ID: 230401942



---

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

**For residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act at [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf) or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For residents of Oregon:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission** - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General** Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General** Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General** - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General** - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General** - Consumer Protection Division: 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General** - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General** - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General** - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)