LYNCH CARPENTER, LLP
Gerald D. Wells III, PA ID No. 88277
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: 412-322-9243
Fax: 412-231-0246
jerry@lcllp.com

BAILEY & GLASSER LLP
Bart D. Cohen, PA ID No. 57606
1622 Locust Street
Philadelphia, PA 19103
Tel: (267) 973-4855
bcohen@baileyglasser.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

PENNSYLVANIA STATE EDUCATION ASSOCIATION,

Defendant.

Civil Action No.: 2025-CV-02411

CONSOLIDATED COMPLAINT - CLASS ACTION

JURY TRIAL DEMANDED

IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	Civil Action No.: 2025-CV-02411

NOTICE TO DEFEND

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 without further notice for any money claimed in the 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 AT ONCE. IF YOU DO NOT HAVE A LAWYER, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER.

IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH INFORMATION ABOUT AGENCIES THAT MAY OFFER LEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

DAUPHIN COUNTY LAWYER REFERRAL SERVICE
213 North Front Street
Harrisburg, PA 17101
(717) 232-7536

NOTICE
CONCERNING MEDIATION ON OF ACTIONS PENDING BEFORE THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY

The Judges of the Court of Common Pleas of Dauphin County believe that mediation of lawsuits is a very important component of dispute resolution. Virtually all lawsuits can benefit in some manner from mediation.

The Court has adopted Dauphin County Local Rule 1001 to encourage the use of mediation. This early alert enables litigants to determine the best time during the life of their lawsuit for a mediation session. The intent of this early alert is to help the parties act upon the requirement to consider good faith mediation at the optimal time.

The Dauphin County Bar Association provides mediation services and can be reached at 717-232-7536. Free mediation sessions for pro bono cases referred by MidPenn Legal Services are available through the DCBA.

A V I S O

USTED HA SIDO DEMANDADO/A EN CORTE. Si usted desea defenderse de las demandas que se presentan más adelante en las siguientes páginas, debe tomar acción dentro de los próximos veinte (20) días después de la notificación de esta Demanda y Aviso radicando personalmente o por medio de un abogado una comparecencia escrita y radicando en la Corte por escrito sus defensas de, y objecciones a, las demandas presentadas aquí en contra suya. Se le advierte de que si usted falla de tomar acción como se describe anteriormente, el caso puede proceder sin usted y un fallo por cualquier suma de dinero reclamada en la demanda o cualquier otra reclamación o remedio solicitado por el demandante puede ser dictado en contra suya por la Corte sin más aviso adicional. Usted puede perder dinero o propiedad u otros derechos omportantes para usted.

USTED DEBE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI USTED NO TIENE UN ABOGADO, LLAME O VAYA A LA SIGUIENTE OFICINA. ESTA OFICINA PUEDE PROVEERLE INFORMACION A CERCA DE COMO CONSEGUIR UN ABOGADO.

SI USTED NO PUEDE PAGAR POR LOS SERVICIOS DE UN ABOGADO, ES POSIBLE QUE ESTA OFICINA LE PUEDA PROVEER INFORMACION SOBRE AGENCIAS QUE OFREZCAN SERVICIOS LEGALES SIN CARGO O BAJO COSTO A PERSONAS QUE CUALIFICAN.

DAUPHIN COUNTY LAWYER REFERRAL SERVICE
213 North Front Street
Harrisburg, PA 17101
(717) 232-7536

An adequate supply of forms containing the bilingual notices required by these Rules shall be furnished by the Dauphin County Bar Association to the office of the Prothonotary and shall be available for use by litigants and their attorneys.

AVISO
REFERENCES A LA MEDIACIÔN DE LAS ACCIONES PENDIENTES ANTES LA CORTE DE SOPLICAS COMUNES DEL CONDADO DE DAUPHIN

Los jueces de la corte de sûplicas comunes del condado de Dauphin creen que la mediaciôn de pleitos es un componente muy importante de la resoluciôn del conflicto. Virtualmente todos los pleitos pueden beneficiar de cierta manera de la mediaciôn.

La code ha adoptado la regla local de condado de Dauphin 1001 para animar el use de la mediaciôn. Esta alarma temprana permite a litigantes determiner la mejor época durante la vida de su pleito para una sesiôn de la mediaciôn. El intento de esta alarma temprana es actuar sobre la mediaciôn de la buena fe en el tiempo óptimo.

La asociaciôn de la barra del condado de Dauphin proporciona servicios de la mediaciôn y se puede alcanzar en 717-232-7536. La sesiôn libre de la mediaciôn para los favorables casos del bono se refinio por MidPenn que los servicios juridicos están disponibles con el DCBA.

An adequate supply of forms containing the bilingual notices required by these Rules shall be furnished by the Dauphin County Bar Association to the Office of the Prothonotary and shall be available for use by litigants and their attorneys.

IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	Civil Action No.: 2025-CV-02411 **CONSOLIDATED COMPLAINT - CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiffs Melanie Hudson ("Hudson"), James Smith ("Smith"), Gregory Eugene Minarchick ("Minarchick"), Tahira Washington ("Washington"), Nicholas Zullo ("Zullo"), and Joseph Paul Yurcho ("Yurcho") (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their undersigned counsel, bring this Consolidated Class Action Complaint against Defendant Pennsylvania State Education Association ("PSEA" or "Defendant"). Plaintiffs allege the following upon information and belief based on and the investigation of counsel, except as to those allegations that specifically pertain to a specific Plaintiff, which are alleged upon personal knowledge as to that specific Plaintiff.

INTRODUCTION

1. Plaintiffs bring this class action lawsuit on behalf of all persons who

entrusted PSEA with sensitive Personally Identifiable Information ("PII")[1] and Protected Health Information ("PHI") that was impacted in a data breach that PSEA publicly disclosed in March 2025 (the "Data Breach").

2. Plaintiffs' claims arise from PSEA's failure to properly secure and safeguard PII and PHI that was entrusted to it, and its accompanying responsibility to store and transfer that information.

3. PSEA is "the largest and most influential public-sector union in Pennsylvania" whose 178,000 members include "teachers, education support professionals, higher education staff, nurses in health care facilities, retired educators, and college students preparing to become teachers."[2]

4. PSEA had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on its affirmative representations to Plaintiffs and Class Members (defined herein), to keep their PII and PHI confidential, safe, secure, and protected from unauthorized disclosure or access.

5. As explained more fully herein, on or around July 6, 2024, PSEA experienced a security incident that impacted its network environment.[3] However, PSEA failed to publicly disclose the Data Breach until nearly eight months later in March of 2025.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] About PSEA, Pennsylvania State Education Association: https://www.psea.org/about-psea/benefits-of-membership (last visited May 19, 2025).

[3] Exhibit 1: Audrey Plassio's Notice Email.

6. As a result of the Data Breach, the following types of PII and PHI of Class Members may have been compromised: full name, date of birth, Social Security number, driver's license or State ID, account number, account pin, security code, password and routing number, payment card number, payment card pin, payment card expiration date, passport number, taxpayer id number, username and password, health insurance information, and medical information.[4]

7. This consolidated action arises from PSEA's failure to take precautions designed to keep individuals' PII and PHI secure. This is because PSEA owed Plaintiffs and Class Members a duty to take all reasonable and necessary measures to keep the PII and PHI collected safe and secure from unauthorized access. PSEA solicited, collected, used, and derived a benefit from the PII and PHI, yet breached its duty by failing to implement or maintain adequate security practices.

8. PSEA, despite having the financial wherewithal and personnel necessary to prevent the Data Breach, nevertheless failed to use reasonable security procedures and practice appropriate to the nature of the sensitive, unencrypted information it maintained for Plaintiffs and Class Members, causing the exposure of Plaintiffs' and Class Members' PII and PHI.

9. As a result of PSEA's inadequate digital security and notice process, Plaintiffs' and Class Members' PII and PHI were exposed to criminals. Plaintiffs and the Class Members have suffered and will continue to suffer injuries including financial losses caused by misuse of their PII and PHI; the loss or diminished value of their PII and PHI

[4] *Id.*

as a result of the Data Breach; lost time associated with detecting and preventing identity theft; and theft of personal and financial information.

10. Plaintiffs bring this action on behalf of all persons whose PII and PHI was compromised as a result of PSEA's failure to: (i) adequately protect the PII and PHI of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of PSEA's inadequate information security practices; (iii) effectively secure hardware containing protected PII and PHI using reasonable and adequate security procedures free of vulnerabilities and incidents; and (iv) timely notify Plaintiffs and Class Members of the Data Breach. PSEA's conduct amounts to at least negligence and violates applicable law.

11. Plaintiffs bring this action individually and on behalf of a Class of similarly situated individuals against PSEA for (i) negligence, (ii) breach of implied contract, (iii) unjust enrichment, and (iv) declaratory judgment.

12. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to PSEA's inadequate data security practices.

PARTIES

I. Plaintiffs

13. Plaintiff Melanie Hudson is an adult individual who at all relevant times has been a citizen of Pennsylvania residing in Collingdale, Pennsylvania, where she intends to remain.

14. Plaintiff James Smith is an adult individual who at all relevant times has been a citizen of Pennsylvania residing in Jersey Shore, Pennsylvania, where he intends to remain.

15. Plaintiff Gregory Eugene Minarchick is an adult individual who at all relevant times has been a citizen of Pennsylvania residing in Decatur, Pennsylvania, where he intends to remain.

16. Plaintiff Tahira Washington is an adult individual who at all relevant times has been a citizen of Pennsylvania residing in Philadelphia, Pennsylvania, where she intends to remain.

17. Plaintiff Nicholas Zullo is an adult individual who at all relevant times has been a citizen of Pennsylvania residing in Hazle Township, Pennsylvania, where he intends to remain.

18. Plaintiff Joseph Paul Yurcho is an adult individual who at all relevant times has been a citizen of Pennsylvania residing in Pittsburgh, Pennsylvania, where he intends to remain.

II. Defendant

19. PSEA is a public union headquartered in Harrisburg, Pennsylvania having its principal place of business located at 400 North 3rd Street, Harrisburg, Pennsylvania 17105.[5]

[5] Contact Us, Pennsylvania State Education Association, https://www.psea.org/contact-us/work-for-pseaX/office-locations/ (last visited May 19, 2025).

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action because the events and conduct giving rise to the claims brought in this Complaint occurred in large part in this County.

21. This Court has personal jurisdiction over PSEA pursuant to 42 Pa. C.S. § 5301 because it is a Pennsylvania domestic corporation with significant business operations and real property located in this County.

22. Venue is proper in this County under Pa. R.C.P. § 1006(a)(1) because of PSEA's operations in this County, and because a substantial part of the events or omissions giving rise to the claim arose here.

FACTUAL ALLEGATIONS

I. Background on Defendant

23. PSEA is a public union that represents teachers, educational support professionals, counselors, curriculum specialists, librarians, health care workers, school nurses, school dental hygienists, school nurses, school psychologists, school social workers, vocational-technical instructors, community college and junior college educators, students and retirees in the Commonwealth of Pennsylvania.

24. According to PSEA's LinkedIn page, "PSEA represents the labor, policy, and professional interests of 178,000 public school teachers and education support professionals, staff in state higher education institutions, nurses in health care facilities, retired educators, and college students preparing to become teachers."[6]

[6] *See* https://www.linkedin.com/company/pennsylvania-state-education-association. (last visited May 19, 2025).

25. PSEA touts itself as the "largest and most influential public sector union in Pennsylvania."[7]

26. Due to the very nature of PSEA's business, it collects and maintains PII and PHI. For example, on its website, PSEA notes that "With PSEA Direct Dues, we're cutting out the middle man [sic] and giving you a faster, safer, and more secure way to directly pay your dues."[8]

27. PSEA made promises and representations to Plaintiffs and Class Members—who are current and former members and employees of PSEA, as well as relatives of PSEA employees—that the PII and PHI collected from them would be kept safe and confidential, and that the privacy of that information would be maintained.[9]

28. For instance, PSEA touted that it "values the trust and privacy of its members and other supporters" and that it "maintain[s] administrative, technical, and physical safeguards designed to (1) ***insure the security and confidentiality*** of your personal information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) ***protect against unauthorized access*** to or use of such information."[10]

---

[7] What exactly is PSEA?, https://www.psea.org/about-psea/benefits-of-membership/ (last visited May 19, 2025).

[8] https://www.psea.org/about-psea/how-to-join/psea-direct-dues (last visited May 19, 2025).

[9] Privacy Policy, Pennsylvania State Education Association, https://www.psea.org/contact-us/privacy-policy/ (last visited May 19, 2025).

[10] *Id.* (emphasis added).

29. Plaintiffs and Class Members provided their PII and PHI to PSEA with the reasonable expectation and mutual understanding that PSEA would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. As a result of collecting and storing the PII and PHI of Plaintiffs and Class Members for its own financial benefit, PSEA had a continuous duty to adopt and employ reasonable measures to protect Plaintiffs' and the Class Members' PII and PHI from disclosure to third parties.

31. Moreover, the collection and retention of this highly sensitive information conferred certain benefits upon PSEA including, but not limited to, allowing it to tout its ever-increasing membership and thus greater influence as a union in Pennsylvania (and thus attract additional members).

32. Indeed, PSEA touts itself as "the largest and most influential public-sector union in Pennsylvania" and notes that one of the benefits of membership is that "members join their voices to protect [their] pensions, salaries, benefits, and working conditions."[11]

33. Despite its duties and obligations to adopt and maintain reasonable cybersecurity safeguards or policies, PSEA has failed to adequately secure and safeguard its systems and networks from a foreseeable and preventable cyberattack.

34. Indeed, as members of the PSEA, Plaintiffs and Class Members reasonably expected that PSEA would engage in sufficient data protection and maintain adequate safeguards that protected their PII and PHI.

[11] About PSEA, Pennsylvania State Education Association: https://www.psea.org/about-psea/benefits-of-membership (last visited May 19, 2025).

II. The Data Breach

35. On or around July 6, 2024, PSEA experienced a security incident that impacted its network environment.[12] Upon detection, PSEA launched an investigation with the assistance of third-party cybersecurity experts to determine the nature and scope of the incident.[13]

36. The investigation determined that an unauthorized third-party gained access to certain files within PSEA's IT network.[14]

37. PSEA then conducted a comprehensive review of the impacted data to determine what information was compromised and identify affected individuals. On February 18, 2025, PSEA completed its review and determined that certain PII and PHI were included in the impacted data.[15]

38. According to PSEA, the "impacted data may include an individual's full name in combination with one or more of the following elements: Date of Birth, Driver's License or State ID, Social Security Number, Account Number, Account PIN, Security Code, Password and Routing Number, Payment Card Number, Payment Card PIN and Payment Card Expiration Date, Passport Number, Taxpayer ID Number, Username and Password, Health Insurance Information and Medical Information."[16]

---

[12] *See* https://www.psea.org/pages-without-a-home/notice-of-data-security-incident/ (last visited May 19, 2025). Upon information and belief, this notice was substantially similar in content to the notice sent to Class Members.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

39. In its notice, PSEA "want[ed] to stress that not all data elements were acquired for every impacted individual."[17]

40. Nevertheless, according to published reports, "[a]lthough the information exposed varied by individual," the Data Breach "included the personal, financial, and health data of 517,487 people."[18]

41. As explained herein, due to the very nature of the information accessed through the Data Breach, Plaintiffs and Class Members are subject to risk of identity theft.

42. This breach was intentional as the ransomware group Rhysida "took credit for the PSEA data breach in September 2024 and listed the labor union on its data leak site."[19]

43. On March 17, 2025, PSEA filed a notice with Maine Attorney General's office and on March 18, 2025 began sending out notice emails to potentially impacted individuals.[20]

44. While PSEA sought to minimize the damage caused by the Data Breach, it cannot and has not denied that there was unauthorized access to the sensitive PII and PHI of Plaintiffs and the Class Members.

---

[17] *Id.*

[18] https://www.cpomagazine.com/cyber-security/data-breach-hits-pennsylvanias-largest-workers-and-teachers-union-psea-impacting-over-500000-people/ (last visited May 19, 2025).

[19] *Id.*

[20] Data Breach Notifications, Pennsylvania State Education Association, Office of the Maine Attorney General: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e44266ce-8099-4d3c-8635-2c5cdb41f24a.html (last visited May 19, 2025).

45. Individuals affected by the Data Breach are, and remain, at risk that their data will be sold or listed on the dark web and, ultimately, illegally used in the future.

46. Upon information and belief, Defendant maintains records of all individuals who were victims of the Data Breach.

III. PSEA's Failure to Prevent, Identify, and Timely Report the Data Breach

47. PSEA admits that an unauthorized third party accessed its IT network.

48. PSEA failed to take necessary precautions or employ adequate measures necessary to protect its computer systems against unauthorized access and keep individuals' PII and PHI secure.

49. The PII and PHI that PSEA allowed to be exposed in the Data Breach is the type of private information that PSEA knew or should have known would be the target of cyberattacks.

50. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[21] PSEA failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' PII and PHI.

51. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate response plan if a breach occurs.[22] Immediate notification to individuals

[21] Protecting Personal Information: A Guide for Business, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited May 19, 2025).

[22] *Id.*

impacted by a data breach is critical so that those impacted can take measures to protect themselves.

52. Here, PSEA waited for more than eight months after the Data Breach occurred to notify impacted individuals. Moreover, as noted above, PSEA indefensibly waited more than five months after the ransomware group Rhysida took credit for the PSEA Data Breach and disclosed said Breach on its data leak site.

IV. PSEA Knew the Risks of Storing Valuable PII and PHI and the Foreseeable Harm to Victims

53. At all relevant times, PSEA knew it was storing valuable and confidential PII and PHI on its systems and would, therefore, be an attractive target for cybercriminals.

54. PSEA 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 was compromised, as well as intrusion into their highly private health information.

55. 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.

56. Moreover, Rhysida—the ransomware group that claimed responsibility for the Data Breach—first surfaced in May 2023. Since that time, it "has claimed numerous high-profile breaches, including the August 2023 Singing River Health System data

breach affecting 900,000 people and the July 2024 City of Columbus, Ohio, cyberattack affecting 500,000 individuals."[23]

57. Further, in August of 2023, "the US Department of Health and Human Services (HHS) also attributed to the Rhysida ransomware gang, which was in its early stages of development, various attacks on the Healthcare and Public Health (HPH) sector."[24]

58. Consequently, in November 2023, the FBI and others issued "a joint cybersecurity advisory about the Rhysida ransomware gang indiscriminately targeting 'education, healthcare, manufacturing, information technology, and government sectors.'"[25]

59. Thus, PSEA knew or should have known that it was a likely target of this or other cybercriminals months before the Data Breach actually occurred. Despite this, upon information and belief, PSEA did nothing to further protect the highly sensitive data it kept.

60. The PII and PHI stolen in the Data Breach have considerable value and constitute 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."[26] PHI, in addition to

---

[23] https://www.cpomagazine.com/cyber-security/data-breach-hits-pennsylvanias-largest-workers-and-teachers-union-psea-impacting-over-500000-people/ (last visited May 19, 2025).

[24] *Id.*

[25] *Id.*

[26] 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/ (last visited May 19, 2025).

being of a highly personal and private nature, can be used for medical fraud and to submit false medical claims for reimbursement.

61. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S.

62. As explained herein, the sheer breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

V. The Harm Caused by the Data Breach Now and Going Forward

63. Victims of data breaches are susceptible to becoming victims of identity theft. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9). When "identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[27]

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions

[27] Prevention and Preparedness, New York State Police, https://troopers.ny.gov/prevention-and-preparedness (last visited May 19, 2025)

further clarify the measures businesses must take to meet their data security obligations.[28]

65. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft.

66. Stolen PII and PHI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal their identities and online activity.

67. When malicious actors infiltrate companies and copy and exfiltrate the sensitive, private information that those companies store, the stolen information often ends up on the dark web where malicious actors buy and sell that information for profit.[29]

68. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had "more than 350,000 listings, many of which offered stolen or fraudulent documents that anyone with the right amount of money could use to assume another identity."[30] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [PII] belonging to victims from countries all over the world."[31] As data breaches continue to reveal, "PII about employees,

---

[28] Federal Trade Commission, Privacy and Security Enforcement: Press Releases, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited May 19, 2025)

[29] Shining a Light on the Dark Web with Identity Monitoring, IdentityForce (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited May 19, 2025).

[30] Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web, Armor (Apr. 3, 2018), https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/.

[31] *Id.*

students or employees and the public are housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[32]

69. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[33] "Fullz" packages, which includes "extra information about the legitimate credit card owner in case" the scammer's "bona fides are challenged when they attempt to use the credit card" are also offered on the dark web.[34]

70. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[35]

71. Further, according to the same report, "[r]apid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[36]

72. PSEA did not rapidly report to Plaintiffs and Class Members that their PII and PHI had been stolen. Instead, PSEA notified impacted people more than eight

---

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] 2019 Internet Crime Report Released, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

[36] *Id.*

months after the Data Breach occurred, and nearly five months after the Data Breach was touted on Rhysida's data leak site—more than sufficient time to for malicious actors to take advantage of the unknowing Plaintiffs and Class Members.

73. Further, due to the nature of cybercrimes, Plaintiffs and Class Members must remain vigilant. This is because cybercriminals can wait months, or longer, before using the stolen information.

74. Indeed, 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 has 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."[37]

75. Even if stolen PII 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 and PHI about the individual, such as names, addresses, email addresses, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

[37] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/assets/gao-07-737.pdf (last visited May 19, 2025).

76. Plaintiffs and Class Members face a real and substantial risk of identity theft given the nature of the highly sensitive and personal information that was compromised in the Data Breach.

77. Indeed, at least some of Plaintiffs' data has already been misused. For example, Plaintiff Minarchick had to change his debit card, credit card, and bank account number due to fraudulent charges appearing on his accounts in January and April of this year. Further, Plaintiff Minarchick believes he receives regular, ongoing spam calls about being approved for loans he never applied for.

78. Similarly, Plaintiff Washington has had multiple fraudulent charges appear on her debit card after the Data Breach. She has spent significant time having her account closed and a new account opened due to the fraudulent charges, as well as having her funds returned.

VI. The Data Breach's Inclusion of PHI is Particularly Significant

79. With respect to the data breaches implicating PHI, a study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[38]

80. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[39]

[38] https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/ (last visited May 19, 2025).

[39] *Id.*

81. 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."[40]

82. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[41]

83. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[42]

84. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online . . .".[43]

85. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false

[40] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited May 19, 2025).

[41] *Id.*

[42] IDExperts, You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows: https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited May 19, 2025).

[43] https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited May 19, 2025).

bills to insurance companies, or even undergo surgery under a false identity.[44] The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[45]

86. As noted above, some of the information that was compromised in the Data Breach included, among other things, "Username and Password, Health Insurance Information and Medical Information." Accordingly, Plaintiffs and Class Members must remain especially vigilant given the highly sensitive nature of the PHI at issue in this Data Breach.

VII. Plaintiffs and Class Members Suffered Damages

87. As a result of the Data Breach, the PII and PHI of Plaintiffs and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiffs and Class Members, or likely to be suffered as a direct result of PSEA's Data Breach, include: (a) theft of their PII and PHI; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress,

[44] Medical Identity Theft: FAQs for Health Care Providers and Health Plans, FTC, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited May 19, 2025).

[45] Justin Klawans, What is medical identity theft and how can you avoid it?, The Week (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid.

nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to PSEA with the mutual understanding that PSEA would safeguard their PII and PHI against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their PII and PHI, which remains in the possession of PSEA, and which is subject to further injurious breaches so long as PSEA fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and PHI.

88. In addition to a remedy for economic harm, Plaintiffs and Class Members maintain an interest in ensuring that their PII and PHI are secure, remain secure, and not subject to further misappropriation and theft.

89. Once PII and PHI are 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, due to PSEA's conduct. Further, the value of Plaintiffs and Class Members' PII and PHI has been diminished by its exposure in the Data Breach.

90. PSEA disregarded the rights of Plaintiffs and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols

and training practices in place to safeguard Plaintiffs' and Class Members' PII and PHI; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

91. The actual and adverse effects to Plaintiffs and Class Members, including the imminent, immediate, and continuing increased risk of harm for identity theft, identity fraud and/or medical fraud directly or proximately caused by PSEA's wrongful actions and/or inaction and the resulting Data Breach require Plaintiffs and Class Members to take affirmative acts to recover their peace of mind and personal security including, without limitation, purchasing credit reporting services, purchasing credit monitoring and/or internet monitoring services, frequently obtaining, purchasing and reviewing credit reports, bank statements, and other similar information, instituting and/or removing credit freezes and/or closing or modifying financial accounts, for which there is a financial and temporal cost. Plaintiffs and other Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

92. Indeed, the experiences of Plaintiffs are illustrative of the harm already suffered as a result of the Data Breach.

93. For example, in addition to the recent fraudulent activity appearing on his accounts, Plaintiff Minarchick has spent dozens of hours monitoring his accounts and taking ameliorative measures discussed above. He also utilizes a credit monitoring service.

94. Plaintiff Smith now locks his debit card when not in use and suffers from an increase in spam or suspicious calls, texts, and emails.

95. Further, Plaintiff Yurcho has anxiety from this Data Breach and, resultingly, checks his accounts "all the time" to ensure no fraudulent activity. In addition, he spoke with his bank about being the potential victim of fraud due to this Data Breach and believes he now receives far more spam emails after the Data Breach.

96. Finally, since being notified of the Data Breach, Plaintiff Zullo has spent over twenty hours monitoring his accounts for suspicious activity. In addition, he has also expended $21 per month for advanced credit monitoring services to monitor his accounts due to the Data Breach.

97. In short, Plaintiffs and Class Members have suffered real and substantial harm and, due to the nature of the Data Breach, are likely to suffer significant harm in the future.

98. Moreover, Plaintiffs and Class Members are also at a continued risk because their information remains in PSEA's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attacks so long as PSEA fails to undertake the necessary and appropriate security and training measures to protect its current and former members' PII and PHI.

A. Plaintiff Melanie Hudson's Experiences

99. Plaintiff Hudson is or was, at all relevant times, a union member of PSEA.

100. Upon information and belief, PSEA obtained Plaintiff Hudson's PII and PHI in the course of conducting its regular business operations.

101. At the time of the Data Breach, PSEA retained Plaintiff Hudson's PII and PHI.

102. Plaintiff Hudson greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Hudson diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

103. PSEA obtained and continues to maintain Plaintiff Hudson's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

104. Plaintiff Hudson received a notice of Data Security Incident, dated March 18, 2025, directly from PSEA via email—over eight months after the breach occurred.

105. As a result of the Data Breach, Plaintiff Hudson made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, contacting Experian to address her credit, and monitoring her financial accounts weekly for any indication of fraudulent activity, which may take years to detect. Plaintiff Hudson has spent approximately an hour dealing with the Data Breach, which is valuable time Plaintiff Hudson otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

106. Plaintiff Hudson suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of

privacy; (ii) theft of her PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PSEA's possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect the PII and PHI.

107. Plaintiff Hudson additionally suffered actual injury in the form of an increase in spam or suspicious phone calls, texts, and emails. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Hudson's life and caused strain on her, which was a direct result of the Data Breach.

108. The Data Breach has also caused Plaintiff Hudson to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

109. As a result of the Data Breach, Plaintiff Hudson anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

110. As a result of the Data Breach, Plaintiff Hudson is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

111. Plaintiff Hudson has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in PSEAs' possession, are protected and safeguarded from future breaches.

B. Plaintiff James Smith's Experiences

112. Plaintiff Smith is or was, at all relevant times, a union member of PSEA.

113. Upon information and belief, PSEA obtained Plaintiff Smith's PII and PHI in the course of conducting its regular business operations.

114. At the time of the Data Breach, PSEA retained Plaintiff Smith's PII and PHI.

115. Plaintiff Smith greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Smith diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source. PSEA obtained and continues to maintain Plaintiff Smith's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

116. Plaintiff Smith received a notice of Data Security Incident, dated March 18, 2025, directly from PSEA via email—over eight months after the breach occurred. As a result of the Data Breach, Plaintiff Smith made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, locking his debit card when not in use, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Smith has spent approximately an hour dealing with the Data Breach, which is valuable time Plaintiff Smith

otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

117. Plaintiff Smith suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PSEA's possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect the PII and PHI.

118. Plaintiff Smith additionally suffered actual injury in the form of an increase in spam or suspicious calls, texts, and emails. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Smith's life and caused strain on his, which was a direct result of the Data Breach.

119. The Data Breach has also caused Plaintiff Smith to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

120. As a result of the Data Breach, Plaintiff Smith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

121. As a result of the Data Breach, Plaintiff Smith is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

122. Plaintiff Smith has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in PSEAs' possession, are protected and safeguarded from future breaches.

C. Plaintiff Gregory Minarchick's Experiences

123. Plaintiff Minarchick is or was, at all relevant times, a union member of PSEA.

124. Upon information and belief, PSEA obtained Plaintiff Minarchick's PII and PHI in the course of conducting its regular business operations.

125. At the time of the Data Breach, PSEA retained Plaintiff Minarchick's PII and PHI.

126. Plaintiff Minarchick greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Minarchick diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

127. PSEA obtained and continues to maintain Plaintiff Minarchick's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

128. Plaintiff Minarchick received a notice of Data Security Incident, dated March 18, 2025, directly from PSEA via email—over eight months after the breach occurred. As a result of the Data Breach, Plaintiff Minarchick made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, replacing his debit and credit card, changing his account number, changing his online passwords, blocking spam callers, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Minarchick has spent significant time dealing with the Data Breach, approximately sixty hours, spent dealing with the fraudulent debit and credit card charges, changing all of his online passwords, blocking spam callers, and monitoring his accounts daily for signs of fraud which is valuable time Plaintiff Minarchick otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

129. Plaintiff Minarchick suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PSEA's

possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect the PII and PHI.

130. Plaintiff Minarchick additionally suffered actual injury in the form of fraudulent and unauthorized charges on his credit and debit cards in approximately December 2024 and April 2025. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Minarchick's life and caused strain on him, which was a direct result of the Data Breach.

131. The Data Breach has also caused Plaintiff Minarchick to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

132. As a result of the Data Breach, Plaintiff Minarchick anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

133. As a result of the Data Breach, Plaintiff Minarchick is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

134. Plaintiff Minarchick has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in PSEAs' possession, are protected and safeguarded from future breaches.

D. Plaintiff Tahira Washington's Experiences

135. Plaintiff Washington is or was, at all relevant times, a union member of PSEA.

136. Upon information and belief, PSEA obtained Plaintiff Washington's PII and PHI in the course of conducting its regular business operations.

137. At the time of the Data Breach, PSEA retained Plaintiff Washington's PII and PHI.

138. Plaintiff Washington greatly values her privacy and is very careful about sharing her sensitive PII and PHI. Plaintiff Washington diligently protects her PII and PHI and takes proactive steps to ensure her PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source.

139. PSEA obtained and continues to maintain Plaintiff Washington's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

140. Plaintiff Washington received a notice of Data Security Incident, dated March 18, 2025, directly from PSEA via email—over eight months after the breach occurred. As a result of the Data Breach, Plaintiff Washington made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, changing debit cards, calling her bank to dispute debit fraud, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Washington has spent significant time dealing with the Data Breach and the fraudulent charges to her debit card and PayPal account, approximately twelve hours, which is valuable time Plaintiff Washington otherwise would have spent on

other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

141. Plaintiff Washington suffered actual injury from having her PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft and misuse of her PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PSEA's possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect the PII and PHI.

142. Plaintiff Washington additionally suffered actual injury in the form of fraudulent charges on her debit card, and an increase in spam calls, texts, and emails following the Data Breach. Specifically, on September 10, 2024, Plaintiff Washington received an email notifying her of four separate fraudulent charges to her debit card for $97.00 each. Next, on May 13, 2025, Plaintiff Washington received an alert that an unauthorized actor attempted to use her PayPal account to purchase $518.48 worth of merchandise at an Altar'd State store located in Ohio. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Washington's life and caused strain on her, which was a direct result of the Data Breach.

143. The Data Breach has also caused Plaintiff Washington to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII and PHI being placed in the hands of criminals.

144. As a result of the Data Breach, Plaintiff Washington anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

145. As a result of the Data Breach, Plaintiff Washington is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

146. Plaintiff Washington has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remain backed up in PSEAs' possession, are protected and safeguarded from future breaches.

E. Plaintiff Nicholas Zullo's Experiences

147. Plaintiff Zullo is or was, at all relevant times, a union member of PSEA.

148. Upon information and belief, PSEA obtained Plaintiff Zullo's PII and PHI in the course of conducting its regular business operations.

149. At the time of the Data Breach, PSEA retained Plaintiff Zullo's PII and PHI.

150. Plaintiff Zullo greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Zullo diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source. PSEA

obtained and continues to maintain Plaintiff Zullo's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

151. Plaintiff Zullo received a notice of Data Security Incident, dated March 18, 2025, directly from PSEA via email—over eight months after the breach occurred. As a result of the Data Breach, Plaintiff Zullo made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach freezing his credit through the three credit bureaus, changing his passwords, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Zullo also pays approximately $21 per month for credit monitoring services as a result of the Data Breach. Plaintiff Zullo has spent significant time dealing with the Data Breach, approximately twenty hours, which is valuable time Plaintiff Zullo otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

152. Plaintiff Zullo suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PSEA's

possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect the PII and PHI.

153. Plaintiff Zullo additionally suffered actual injury in the form of an increase in spam calls and emails. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Zullo's life and caused strain on him, which was a direct result of the Data Breach.

154. The Data Breach has also caused Plaintiff Zullo to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

155. As a result of the Data Breach, Plaintiff Zullo anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

156. As a result of the Data Breach, Plaintiff Zullo is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

157. Plaintiff Zullo has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in PSEAs' possession, are protected and safeguarded from future breaches.

F. Plaintiff Joseph Yurcho's Experiences

158. Plaintiff Yurcho is or was, at all relevant times, a union member of PSEA.

159. Upon information and belief, PSEA obtained Plaintiff Yurcho's PII and PHI in the course of conducting its regular business operations.

160. At the time of the Data Breach, PSEA retained Plaintiff Yurcho's PII and PHI.

161. Plaintiff Yurcho greatly values his privacy and is very careful about sharing his sensitive PII and PHI. Plaintiff Yurcho diligently protects his PII and PHI and takes proactive steps to ensure his PII and PHI are kept safe and secure and stores any documents containing PII and PHI in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII or PHI over the Internet or any other unsecured source. PSEA obtained and continues to maintain Plaintiff Yurcho's PII and PHI and has a continuing legal duty and obligation to protect that PII and PHI from unauthorized access and disclosure.

162. Plaintiff Yurcho received a notice of Data Security Incident, dated March 18, 2025, directly from PSEA via email—over eight months after the breach occurred. As a result of the Data Breach, Plaintiff Yurcho made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, speaking with his bank to alert them to potential fraud, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Yurcho has spent significant time dealing with the Data Breach, which is valuable time Plaintiff Yurcho otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

163. Plaintiff Yurcho suffered actual injury from having his PII and PHI compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his PII and PHI; (iii) lost or diminished value of PII and PHI; (iv) lost time and opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in PSEA's possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect the PII and PHI.

164. Plaintiff Yurcho suffers from anxiety as a result of his PII and PHI being exposed in the Data Breach. The actions by unauthorized criminal third parties have detrimentally impacted Plaintiff Yurcho's life and caused strain on him, which was a direct result of the Data Breach.

165. The Data Breach has also caused Plaintiff Yurcho to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII and PHI being placed in the hands of criminals.

166. As a result of the Data Breach, Plaintiff Yurcho anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

167. As a result of the Data Breach, Plaintiff Yurcho is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

168. Plaintiff Yurcho has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remain backed up in PSEA's possession, are protected and safeguarded from future breaches.

CLASS ALLEGATIONS

169. Plaintiffs bring this class action pursuant to Rules 1702, 1708 and 1709 of the Pennsylvania Rules of Civil Procedure, individually and on behalf of the following Class.

> All persons whose PII and/or PHI was compromised as a result of the Data Breach publicly announced by PSEA in March 2025 (the "Class").

170. Specifically excluded from the Class are PSEA, its officers, directors, agents, trustees, parents, children, corporations, trusts, representatives, principals, partners, joint venturers, or entities controlled by PSEA, and their heirs, successors, assigns, or other persons or entities related to or affiliated with PSEA and/or their officers and/or directors, the judge assigned to this action, and any member of the judge's immediate family.

171. The members of the Class are referred to as "Class Members."

172. Plaintiffs reserve the right to amend the Class definitions above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

173. This action may be certified as a class action under Pa.R.C.P. 1702 because it satisfies the numerosity, commonality, typicality, adequacy, and superiority requirements therein.

174. Numerosity – Pa.R.C.P. 1702(1): The Class is so numerous that joinder of all Class Members is impracticable. Upon information and belief, Plaintiffs estimates that the Class is comprised of several hundred thousand Class Members. The Class is sufficiently numerous to warrant certification.

175. Commonality – Pa.R.C.P. 1702(2): This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether and to what extent PSEA had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether PSEA was negligent in collecting and storing Plaintiffs' and Class Members' PII, and breached its duties thereby;

c. Whether PSEA took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII;

d. Whether PSEA failed to adequately safeguard Plaintiffs' and Class Members' PII;

e. Whether PSEA breached its duty to exercise reasonable care in handling Plaintiffs' and Class Members' PII;

f. Whether PSEA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

g. Whether Plaintiffs and Class Members are entitled to damages as a result of PSEA's wrongful conduct; and

h. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

176. Typicality – Pa.R.C.P. 1702(3): Plaintiffs' claims are typical of the claims of Class Members. Plaintiffs' and Class Members' claims are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and Class Members each had their PII exposed and/or accessed by an unauthorized third party.

177. Adequacy of Representation – Pa.R.C.P. 1702(4) and 1709: Plaintiffs are an adequate representative of the Class. Plaintiffs will fairly, adequately, and vigorously represent and protect the interests of the Class Members and have no interests antagonistic to the Class Members. In addition, Plaintiffs have retained counsel who are

competent and experienced in the prosecution of class action litigation. The claims of Plaintiffs and the Class Members are substantially identical, as explained above.

178. Predominance – Pa.R.C.P. 1708(a)(1): Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, PSEA's liability and the fact of damages are common to Plaintiffs and each member of the Class. If PSEA breached its duty to Plaintiffs and Class Members, then Plaintiffs and each Class member suffered damages by that conduct.

179. Manageability – Pa.R.C.P. 1708(a)(2): While the precise size of the Class is unknown without the disclosure of PSEA's records, PSEA has indicated that the number of individuals impacted is approximately 500,000. The claims of Plaintiffs and the Class members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and the Class.

180. Risk of Inconsistent, Varying or Prejudicial Adjudications – Pa.R.C.P. 1708(a)(3): If the claims of Plaintiffs and the members of the Class were tried separately, PSEA may be confronted with incompatible standards of conduct and divergent court decisions. Furthermore, if the claims of Plaintiffs and the members of the Class were tried individually, adjudications with respect to individual Class members and the propriety of their claims could be dispositive on the interests of other members of the Class not party

to those individual adjudications and substantially, if not fully, impair or impede their ability to protect their interests.

181. Litigation Already Commenced – Pa.R.C.P. 1708(a)(4): To Plaintiffs' knowledge, all individually filed actions have been consolidated before this Court.

182. The Appropriateness of the Forum – Pa.R.C.P. 1708(a)(5): This is the most appropriate forum to concentrate the litigation because the PSEA resides in this County.

183. The Class Members' Claims Support Certification – Pa.R.C.P. 1708(a)(6) and (7): Given the relatively low amount recoverable by each Class member, the expenses of individual litigation are insufficient to support or justify individual suits. Furthermore, the damages that may be recovered by the Class will not be so small such that class certification is unjustified.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and Class Members)

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

185. PSEA owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting the PII and PHI it collected from them as a condition of their dealings with PSEA from being compromised, lost, stolen, accessed and misused by unauthorized parties. This duty includes, among other things, designing, maintaining, overseeing, and testing PSEA's security systems to ensure that PII and PHI in PSEA's possession was adequately secured and protected.

186. PSEA owed a duty of care to Plaintiffs and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII and PHI of its members, employees, and their dependents and beneficiaries.

187. PSEA had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust PSEA with their PII and PHI as a condition of membership or employment was predicated on the understanding that PSEA would take adequate security precautions to protect their PII and PHI.

188. PSEA owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of inadequate security practices. PSEA knew or should have known it was a target of cyberattacks and the critical importance of adequately securing its members' and employees' PII and PHI.

189. Plaintiffs and members of the Class entrusted PSEA with their PII and PHI with the understanding that PSEA would safeguard their information, as well as the information of their dependents and beneficiaries.

190. PSEA's conduct also created a foreseeable risk of harm to Plaintiffs and Class Members by failing to: (1) secure its systems and exercise adequate oversight of its data security protocols; (2) ensure compliance with industry standard data security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

191. PSEA knew, or should have known, of the risks inherent in collecting and storing PII and PHI, the vulnerabilities of its systems, and the importance of adequate

security. PSEA was aware of numerous, well-publicized data breaches in the months and years preceding the Data Breach.

192. PSEA breached its common law duty to act with reasonable care in collecting and storing the PII and PHI of its members, employees, and their dependents and beneficiaries, which exists independently from any contractual obligations between the parties. Specifically, PSEA breached its common law, statutory, and other duties to Plaintiffs and Class Members in numerous ways, including by:

a. failing to adopt reasonable data security measures, practices, and protocols;

b. failing to implement data security systems, practices, and protocols sufficient to protect Plaintiffs' and Class Members' PII and PHI;

c. storing former members' and employees' PII and PHI longer than reasonably necessary;

d. failing to comply with industry-standard data security measures; and

e. failing to timely disclose critical information regarding the nature of the Data Breach.

193. PSEA's failure to implement and maintain adequate data security measures to protect Plaintiffs' and Class Members' PII and PHI created conditions conducive to a foreseeable, intentional criminal act in the form of the Data Breach. Plaintiffs and Class Members did not contribute to the Data Breach or the subsequent misuse of their PII and PHI as described herein.

194. In addition, violations of statutes which establish a duty to take precautions to protect a particular class of persons from a particular injury or type of injury may constitute negligence *per se*.

195. Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as PSEA, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of PSEA's duty in this regard.

196. PSEA violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' PII and PHI and not complying with applicable industry standards, as described in detail herein. PSEA's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

197. PSEA's violation of Section 5 of the FTC Act constitutes negligence *per se*.

198. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

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

200. As a direct and proximate result of PSEA's conduct, Plaintiffs and Class Members have and will suffer damages including, but not limited to: (i) the loss of value of their PII and PHI and loss of opportunity to determine for themselves how their PII and PHI is used; (ii) the publication and/or theft of their PII and PHI; (iii) out-of-pocket

expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with 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) time, effort, and expense associated with placing fraud alerts or 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 and PHI, which remains in PSEA's possession and is subject to further unauthorized disclosures so long as PSEA fails to undertake appropriate and adequate measures to protect it; 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 and PHI for the rest of their lives.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and Class Members)

201. Plaintiffs re-allege the above allegations as if fully set forth herein.

202. In connection with receiving services from PSEA, Plaintiffs and Class Members entered into implied contracts with PSEA.

203. When Plaintiffs and Class Members paid money and provided their PII and PHI to PSEA, either directly or indirectly, as a pre-condition and in exchange for goods or services, they entered into implied contracts with PSEA.

204. Pursuant to these implied contracts, in exchange for the consideration and PII and PHI provided by Plaintiffs and Class Members, PSEA agreed to, among other things, and Plaintiffs and Class Members understood that PSEA would: (1) provide

products and/or services to Plaintiffs and Class Members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiffs' and Class Members' PII and PHI; and (3) protect Plaintiffs' and Class Members' PII and PHI in compliance with federal and state laws and regulations and industry standards.

205. The protection of PII and PHI was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and PSEA, on the other hand. Indeed, as set forth herein, PSEA recognized its duty to provide adequate data security and ensure the privacy of its members' and employees' PII and PHI with its practice of providing a privacy policy on its website.

206. Plaintiffs and Class Members performed their obligations under the implied contract when they provided PSEA with their PII and PHI.

207. Had Plaintiffs and Class Members known that PSEA would not adequately protect its members' and employees' PII and PHI, they would have limited their disclosures of PII and PHI to PSEA, or chosen not to do business with PSEA.

208. PSEA breached its obligations under its implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards.

209. PSEA's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and Class Members have suffered from the Data Breach.

210. Plaintiffs and Class Members suffered by virtue of PSEA's breach of their implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (vi) they have lost time and incurred expenses, and will incur future costs to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) the have overpaid for the services they received without adequate data security.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and Class Members)

211. Plaintiffs re-allege the above allegations as if fully set forth herein.

212. This count is plead in the alternative to the breach of implied contract count above.

213. By its wrongful acts and omissions described herein, PSEA has obtained a benefit by unduly taking advantage of Plaintiffs and Class Members.

214. PSEA, prior to and at the time Plaintiffs and Class Members entrusted it with their PII and PHI, caused Plaintiffs and Class Members to reasonably believe that it would keep that PII and PHI secure.

215. PSEA was aware, or should have been aware, that reasonable consumers would want their PII and PHI kept secure, and would have limited their disclosures of PII

and PHI to PSEA, or not contracted with PSEA, directly or indirectly, had they known that PSEA's information systems were sub-standard for that purpose.

216. PSEA was also aware that, if the sub-standard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiffs' and Class Members' decisions to seek services from it.

217. PSEA failed to disclose facts pertaining to its substandard information systems, or defects and vulnerabilities therein before Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information from PSEA.

218. Instead, PSEA suppressed and concealed such information. By concealing and suppressing that information, PSEA denied Plaintiffs and Class Members the ability to make rational and informed purchasing and servicing decisions, and took undue advantage of Plaintiffs and Class Members.

219. PSEA was unjustly enriched at the expense of Plaintiffs and Class Members, as PSEA derived revenue, benefits, and compensation, in part, at the expense of Plaintiffs and Class Members; however, Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and services that did not satisfy the purposes for which they paid.

220. Since PSEA's realized benefits and compensation from these transactions improperly, PSEA is not legally or equitably entitled to retain those benefits or that compensation.

221. Plaintiffs and Class Members seek an Order of this Court requiring PSEA to refund, disgorge, and pay as restitution any profits obtained by PSEA from its wrongful

conduct, or establishing a constructive trust from which Plaintiffs and Class Members may seek restitution.

COUNT IV
DECLARATORY AND INJUNCTIVE RELIEF
PENNSYLVANIA DECLARATORY JUDGMENTS ACT, 42 PA.C.S.A. § 7531
(On Behalf of Plaintiffs and Class Members)

222. Plaintiffs re-allege the above allegations as if fully set forth herein.

223. This cause of action is brought under the Pennsylvania Declaratory Judgments Act, 42 Pa.C.S.A. § 7531.

224. As previously alleged, Plaintiffs and Class Members entered into contracts that required PSEA to provide adequate security for the PII and PHI it collected from them.

225. PSEA owes a duty of care to Plaintiffs and Class Members requiring it to adequately secure PII and PHI.

226. PSEA still possesses Plaintiffs' and Class Members' PII and PHI.

227. Since the Data Breach, PSEA has announced no specific changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which allowed the Data Breach to occur and, thereby, prevent further attacks.

228. PSEA has not satisfied its contractual obligations and legal duties to Plaintiffs and Class Members. In fact, now that PSEA's insufficient data security is known to hackers, the PII and PHI in PSEA's possession is even more vulnerable to cyberattack.

229. Actual harm has arisen in the wake of the Data Breach regarding PSEA's contractual obligations and duties of care to provide adequate security measures to Plaintiffs and Class Members. In addition, Plaintiffs and Class Members are at risk of

additional or further harm due to the exposure of their PII and PHI and PSEA's failure to address the security failings that lead to such exposure.

230. There is no reason to believe that PSEA's security measures are any more adequate now than they were before the Data Breach or in compliance with PSEA's contractual obligations and legal duties.

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

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on PSEA's systems on a periodic basis, and promptly correcting any problems or issues detected by such third-party security auditors;

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

c. auditing, testing, and training its security personnel with respect to any new or modified procedures;

d. segmenting Plaintiffs' and Class Members' PII and PHI by, among other things, creating firewalls and access controls so that if one area of PSEA's system is compromised, hackers cannot gain access to other portions of its systems;

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

f. conducting regular computer system scanning and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel as to how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. meaningfully educating its current, former, and prospective members and employees about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an Order certifying this action as a class action, appointing Plaintiffs as class representatives for the Class, and appointing Interim Co-Lead Counsel to represent the Class;

b. For equitable relief enjoining PSEA from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' PII and PHI, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c. For equitable relief compelling PSEA to utilize appropriate methods and policies with respect to member and employee data collection, storage, and safety, and to disclose with specificity the types of PII and PHI compromised as a result of the Data Breach;

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

e. Ordering PSEA to pay for not less than ten years of credit monitoring services for Plaintiffs and Class Members;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: May 19, 2025

Respectfully submitted,

/s/ Gerald D. Wells III

LYNCH CARPENTER
Gerald D. Wells III, PA ID No. 88277
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
jerry@lcllp.com

BAILEY & GLASSER LLP
Bart D. Cohen, PA ID No. 57606
1622 Locust Street
Philadelphia, PA 19103
Tel: (267) 973-4855
bcohen@baileyglasser.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

SHUB JOHNS & HOLBROOK LLP
Benjamin F. Johns, PA ID No. 201373
Samantha E. Holbrook, PA ID No. 311829
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
bjohns@shublawyers.com
sholbrook@shublawyers.com

LEVI & KORSINSKY, LLP
Courtney E. Maccarone*
Melissa G. Meyer*
33 Whitehall Street, 17th Floor
New York, NY 10004
Tel: (212) 363-7500
Fax: (212) 363-7171
cmaccarone@zlk.com
mmeyer@zlk.com

LEVIN SEDRAN & BERMAN LLP
Charles E. Schaffer, PA ID No. 76259
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
Gary Klinger*
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel: (866) 252-0878
gklinger@milberg.com

AHDOOT & WOLFSON, PC
Andrew W. Ferich, PA ID No. 313696
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
aferich@ahdootwolfson.com

EDELSON LECHTZIN LLP
Marc H. Edelson, PA ID No. 51834
411 S. State Street, Suite N300
Newtown, PA 18940
Tel: (215) 867-2399
medelson@edelson-law.com

Plaintiffs' Executive Committee

**pro hac vice* forthcoming

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	**IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA** Civil Action No.: 2025-CV-02411 **VERIFICATION OF PLAINTIFF MELANIE HUDSON**

VERIFICATION

I, Melanie Hudson, hereby state:

1. I am a plaintiff in this action;

2. I verify that the statements made in the foregoing Consolidated Complaint are true and correct to the best of my knowledge, information, and belief; and

3. I understand that the statements in said Consolidated Complaint are subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

DATED: 05 / 19 / 2025

Melanie Hudson

Melanie Hudson

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	**IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA** Civil Action No.: 2025-CV-02411 **VERIFICATION OF PLAINTIFF JAMES SMITH**

VERIFICATION

I, James Smith, hereby state:

1. I am a plaintiff in this action;

2. I verify that the statements made in the foregoing Consolidated Complaint are true and correct to the best of my knowledge, information, and belief; and

3. I understand that the statements in said Consolidated Complaint are subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

DATED: 05 / 19 / 2025

James Smith

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	**IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA** Civil Action No.: 2025-CV-02411 **VERIFICATION OF PLAINTIFF GREGORY EUGENE MINARCHICK**

VERIFICATION

I, Gregory Eugene Minarchick, hereby state:

1. I am a plaintiff in this action;

2. I verify that the statements made in the foregoing Consolidated Complaint are true and correct to the best of my knowledge, information, and belief; and

3. I understand that the statements in said Consolidated Complaint are subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

DA TED: 05 / 19 / 2025

Gregory Eugene Minarchick

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	**IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA** Civil Action No.: 2025-CV-02411 **VERIFICATION OF PLAINTIFF TAHIRA WASHINGTON**

VERIFICATION

I, Tahira Washington, hereby state:

1. I am a plaintiff in this action;

2. I verify that the statements made in the foregoing Consolidated Complaint are true and correct to the best of my knowledge, information, and belief; and

3. I understand that the statements in said Consolidated Complaint are subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

DA TED: 5/19/2025

DocuSigned by:
51BC1B679D294DF...
Tahira Washington

MELANIE HUDSON, JAMES SMITH, GREGORY MINARCHICK, TAHIRA WASHINGTON, NICHOLAS ZULLO, and JOSEPH YURCHO, individually and on behalf of all others similarly situated, Plaintiffs, v. PENNSYLVANIA STATE EDUCATION ASSOCIATION, Defendant.	**IN THE COURT OF COMMON PLEAS OF DAUPHIN COUNTY, PENNSYLVANIA** Civil Action No.: 2025-CV-02411 **VERIFICATION OF PLAINTIFF NICHOLAS ZULLO**

VERIFICATION

I, Nicholas Zullo, hereby state:

1. I am a plaintiff in this action;

2. I verify that the statements made in the foregoing Consolidated Complaint are true and correct to the best of my knowledge, information, and belief; and

3. I understand that the statements in said Consolidated Complaint are subject to the penalties of 18 Pa.C.S. § 4904 relating to unsworn falsification to authorities.

DA TED: 5/19/2025

Signed by:
Nicholas Zullo
9C540F9EB8814B5...

Nicholas Zullo

VERIFICATION

I, Joseph Paul Yurcho hereby states that I am one of the Plaintiffs in this action and verifies that the statements made in the Consolidated Complaint are true and correct to the best of his/her knowledge, information and belief.

The undersigned understands that the statements therein are made subject to penalties of 18 Pa. C.S. Section 4904 relating to unsworn falsification to authorities.

Joseph Yurcho (May 19, 2025 17:35 EDT)

Joseph Paul Yurcho

Date: 05/19/2025

CERTIFICATE OF COMPLIANCE

I certify that this filing complies with the provisions of the Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts that require filing confidential information and documents differently than non-confidential information and documents.

/s/ Gerald D. Wells, III
Gerald D. Wells, III

EXHIBIT 1

Gmail [redacted]

Notice of Data Security Incident

1 message

Aaron Chapin, PSEA President <noreply@psea.org> Tue, Mar 18, 2025 at 7:37 PM
To: [redacted]@gmail.com

PENNSYLVANIA STATE EDUCATION ASSOCIATION

Notice of Data Security Incident

Pennsylvania State Education Association ("PSEA") is providing notice regarding a recent data security incident. The privacy and security of the protected personal information entrusted to us is of the utmost importance to PSEA. As such, we wanted to provide impacted individuals with information about the incident, explain the services available to the impacted individuals, and let them know that we continue to take significant measures to protect the personal information entrusted to us.

What Happened?

PSEA experienced a security incident on or about July 6, 2024 that impacted our network environment. Through a thorough investigation and extensive review of impacted data which was completed on February 18, 2025, we determined that the data acquired by the unauthorized actor contained some personal information belonging to individuals whose information was contained within certain files within our network. We took steps, to the best of our ability and knowledge, to ensure that the data taken by the unauthorized actor was deleted. We want to make the impacted individuals aware of the incident and provide them with steps they can take to further protect their information.

What We Are Doing.

Upon learning of the issue, we commenced a prompt and thorough investigation. As part of our investigation, we have worked closely with external cybersecurity professionals and notified law enforcement of the incident. Additionally, PSEA is reviewing its existing policies and training protocols relating to data protection while enhancing security measures and monitoring tools to further mitigate risks of this nature. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of the protected personal information entrusted to us.

What Information Was Involved?

We want to stress that not all data elements were acquired for every impacted individual. However, the impacted data may include an individual's full name in combination with one or more of the following elements: Date of Birth, Driver's License or State ID, Social Security Number, Account Number, Account PIN, Security Code, Password and Routing Number, Payment Card Number, Payment Card PIN and Payment Card Expiration Date, Passport Number, Taxpayer ID Number, Username and Password, Health Insurance Information and Medical Information.

What You Can Do.

We have no evidence that any of the information has been used for identity theft or to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make the impacted individuals aware of the incident.

The individuals who had their Social Security number impacted will be provided with access to credit monitoring and identity restoration services, through IDX, free of charge. To enroll in credit monitoring, please

call IDX at 1-877-720-5373 or go to https://app.idx.us/account-creation/protect. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. The impacted individuals have until June 17, 2025 to enroll in the services offered.

Below there is also information on precautionary measures that individuals may take to protect their personal information, including placing a fraud alert and/or security freeze on credit files and/or obtaining a free credit report. Additionally, individuals should always remain vigilant by reviewing their financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of protected personal information in our possession and have taken precautions to safeguard it.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-877-720-5373. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time, excluding holidays. This response line is staffed with professionals familiar with this incident and knowledgeable on what impacted individuals can do to help protect against potential misuse of their information.

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert on Your Credit File.**

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	***Experian***	***TransUnion***
P.O. Box 105069	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348-5069	Allen, TX 75013	P.O. Box 2000
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	www.experian.com/fraud/center.html	Chester, PA 19016-2000
(800) 525-6285	(888) 397-3742	www.transunion.com/fraud-alerts
		(800) 680-7289

2. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax	***Experian***	***TransUnion***
P.O. Box 105069	P.O. Box 9554	Fraud Victim Assistance Department
Atlanta, GA 30348-5069	Allen, TX 75013	P.O. Box 2000
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	www.experian.com/fraud/center.html	Chester, PA 19016-2000
(800) 525-6285	(888) 397-3742	www.transunion.com/fraud-alerts
		(800) 680-7289

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit

monitoring service, you may refreeze your credit file.

3. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify that all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you receive notice that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

5. **Protecting Your Medical Information.**

We have no information to date indicating that medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

6. **State Specific Information.**

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA) which include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), or TTY: 1-866-653-4261.

---

400 N. 3rd Street, Harrisburg, PA 17101