
		New Jersey Judiciary Civil Practice Division Civil Case Information Statement (CIS)		
Use for initial Law Division Civil Part pleadings (not motions) under Rule 4:5-1. Pleading will be rejected for filing, under Rule 1:5-6(c), if information above the black bar is not completed, or attorney's signature is not affixed.				
For Use by Clerk's Office Only				
Payment type <input type="checkbox"/> check <input type="checkbox"/> charge <input type="checkbox"/> cash	Charge/Check Number	Amount \$	Overpayment \$	Batch Number
Attorney/Pro Se Name Kenneth J. Grunfeld, Esq.		Telephone Number (215) 985-9177 ext.2005		County of Venue Bergen
Firm Name (if applicable) GOLOMB SPIRT GRUNFELD, P.C.			Docket Number (when available)	
Office Address - Street 1835 Market Street, Suite 2900		City Philadelphia	State PA	Zip 19103
Document Type Complaint			Jury Demand <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
Name of Party (e.g., John Doe, Plaintiff) Victor Mateo		Caption Victor Mateo v. SEIU		
Case Type Number (See page 3 for listing) <u>508</u>				
Are sexual abuse claims alleged?			<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Does this case involve claims related to COVID-19?			<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Is this a professional malpractice case? If "Yes," see N.J.S.A. 2A:53A-27 and applicable case law regarding your obligation to file an affidavit of merit.			<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Related Cases Pending? If "Yes," list docket numbers			<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Do you anticipate adding any parties (arising out of same transaction or occurrence)?			<input type="checkbox"/> Yes	<input checked="" type="checkbox"/> No
Name of defendant's primary insurance company (if known)			<input type="checkbox"/> None	<input checked="" type="checkbox"/> Unknown

The Information Provided on This Form Cannot be Introduced into Evidence.	
Case Characteristics for Purposes of Determining if Case is Appropriate for Mediation	
Do parties have a current, past or recurrent relationship? <input checked="" type="checkbox"/> Yes <input type="checkbox"/> No	
If "Yes," is that relationship:	
<input type="checkbox"/> Employer/Employee <input type="checkbox"/> Friend/Neighbor <input type="checkbox"/> Familial <input type="checkbox"/> Business <input checked="" type="checkbox"/> Other (explain) <u>Union/Union Member</u>	
Does the statute governing this case provide for payment of fees by the losing party? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	
Use this space to alert the court to any special case characteristics that may warrant individual management or accelerated disposition. Putative class action regarding a data breach	
♿ Do you or your client need any disability accommodations? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, please identify the requested accommodation:	
Will an interpreter be needed? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No If yes, for what language?	
I certify that confidential personal identifiers have been redacted from documents now submitted to the court and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b).	
Attorney/Self-Represented Litigant Signature: 	

BY: **KENNETH J. GRUNFELD, ESQUIRE**

Attorney I.D. No. 026091999

KEVIN FAY, ESQUIRE

Attorney I.D. No. 005692010

GOLOMB SPIRT GRUNFELD, P.C.

1835 Market Street

Suite 2900

Philadelphia, PA 19103

(215) 985-9177

Attorneys for Plaintiff and the Class

VICTOR MATEO, on behalf of himself
and all others similarly situated,

Plaintiff,

vs.

SERVICE EMPLOYEES
INTERNATIONAL UNION, LOCAL
32BJ.

Defendant.

**SUPERIOR COURT OF NEW JERSEY
LAW DIVISION: BERGEN COUNTY**

DOCKET NO.

CASE CODE: ____

CIVIL ACTION

**CLASS ACTION COMPLAINT
DEMAND FOR JURY TRIAL**

Plaintiff Victor Mateo (“Plaintiff”), individually and on behalf of the Class defined below of similarly situated persons, brings this Class Action Complaint and alleges the following against Service Employees International Union, Local 32BJ (“SEIU 32BJ” or “Defendant”), based upon personal knowledge with respect to Plaintiff and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

NATURE OF THE ACTION

1. This is a consumer class action lawsuit brought by Plaintiff, individually and on behalf of all others similarly situated (i.e., the Class Members), who are current or former members and employees of SEIU 32BJ and entrusted it to safeguard their personally identifiable information (“PII”), which includes without limitation names, dates of birth and Social Security numbers. SEIU

32BJ has failed to comply with industry standards to protect information in systems that contain that PII, and has failed to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised. Plaintiff seeks, among other things, orders requiring SEIU 32BJ to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future.

2. In February of 2022, SEIU 32BJ announced a data security incident that occurred between October 21, 2021 and November 1, 2021 involving its employees and members' PII (the "Data Breach"). As a result, an unauthorized party accessed certain files and folders within the Defendant's systems and may have viewed or acquired data containing affected parties' names, addresses and Social Security numbers, among other potentially damaging PII. The security incident was wide-reaching, effecting a number of the organization's computer systems and compromising the PII of up to 230,487 people.

3. SEIU 32BJ began mailing notice letters to those whose information was compromised on or around February 11, 2022 and upon information and belief, continued its investigation of the incident.

4. As a result of SEIU 32BJ's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members now and will forever face a substantial increased risk of identity theft. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to the Defendant's failures.

5. Accordingly, Plaintiff, individually and on behalf of all others similarly situated, alleges claims for negligence and negligence *per se*, violations of the New Jersey Consumer Fraud

Act and injunctive/declaratory relief.

PARTIES

6. Plaintiff Victor Mateo is a citizen and resident of New Jersey. At all times relevant to this Complaint, Plaintiff is a former member of SEIU 32BJ whose PII was collected and maintained by SEIU 32BJ and disclosed without authorization to an unknown and unauthorized third party as a result of the Data Breach.

7. Defendant SEIU 32BJ is the largest union of property service workers in the U.S. See <https://www.seiu32bj.org/> (last visited June 27, 2022). SEIU 32BJ claims to have over 175,000 current members who are principally located in the northeastern states, including in New Jersey, which has its own district of members. *Id.* at <https://www.seiu32bj.org/32bj-constitution/>. Its principal address is located at 25 West 18th Street, New York, NY 10011 (the Manhattan Office and Union Headquarters). Due to the nature of the services it provides, SEIU 32BJ acquires and electronically stores members' and employees' PII.

JURISDICTION AND VENUE

8. The Court has jurisdiction over Plaintiff's claims because it is an action for damages that exceeds the jurisdictional minimum of this Court and because at all relevant times, Plaintiff resided in the State of New Jersey ("New Jersey"), Defendant conducted (and continues to conduct) substantial business in New Jersey and the Data Breach at issue impacted the Plaintiff's PII.

9. Venue is proper in this County pursuant to Rule 4:3-2 in that Plaintiff resides in Bergen County, Defendant does business in Bergen County, and because a substantial part of the events giving rise to this action as it relates to the Plaintiff occurred in Bergen County.

BACKGROUND AND FACTS

10. Defendant SEIU 32BJ was established in 1934 and is the is the largest union of property service workers in the U.S. with over 175,000 current members. *See* <https://www.seiu32bj.org/> (last visited June 27, 2022). SEIU 32BJ members are principally located in the northeastern United States, including in New Jersey. *Id.*

11. In February of 2022, Defendant publicly disclosed that an unauthorized party “may have acquired data containing certain employee and member information.” *See* Letter page 1, attached hereto as Exhibit 1. Defendant confirmed that “a limited number” of 32BJ computer systems experienced this data security incident. *Id.*

12. Defendant initiated an investigation and engaged cybersecurity experts to determine the size and scope of the breach. It learned that between October 21, 2021 and November 1, 2021 there was a data security incident involving its employees’ and members’ PII. *Id.*

13. SEIU 32BJ then conducted a review of its files to see if any “sensitive information” was impacted. *Id.* The review was completed on January 13, 2022 and it was determined that in fact, members and employees’ PII, including the Plaintiff’s PII, was put at risk, including names, dates of birth and Social Security numbers. The security incident was wide-reaching, affecting a number of the organization’s computer systems and compromising the PII of up to 230,487 people.

14. Defendant mailed notification letters to all affected individuals informing them about the Data Breach. In these letters, Defendants offered affected individuals the opportunity to enroll in free credit monitoring and identity restoration services through a product sold by Equifax.

15. The Notification Letters were untimely and deficient as a matter of law, failing to provide basic details concerning the Data Breach, including, but not limited to, why sensitive information was stored on systems without adequate security, the deficiencies in the security

systems that permitted unauthorized access, whether the stolen data was encrypted or otherwise protected, and whether it knows if the data has not been further disseminated. *Id.*

16. Further, SEIU 32BJ's efforts to protect those affected were limited to the letter. SEIU 32BJ has a number of ways to communicate with its current and former members and employees, yet it took no steps to do so other than through the one notice letter. Upon information and belief, Defendant did not post notices in District locations, provide training or information to union leaders, run programs for current members and/or employees, or do anything to encourage those impacted to sign up for the credit monitoring and identity restoration services product.

17. In deliberate disregard of the fact that the stolen sensitive information was accessed by an unauthorized third party, SEIU 32BJ downplayed the seriousness of the incident by failing to take steps necessary to inform Plaintiff and Class Members that their data was in fact stolen by third party bad actors rather than saying it "*may have been* viewed or acquired." and that SEIU 32BJ, seemingly more out of an abundance of caution, wanted to make Plaintiff and Class Members aware of the Data Breach.

18. SEIU 32BJ acknowledges that it is responsible to safeguard Plaintiff and Class Members' PII. It pledges that it takes privacy very seriously and makes numerous promises that it will maintain the security and privacy of PII.

19. On July 23, 2021, SEIU 32BJ updated its Privacy Policy. *See* <https://www.32bjfunds.org/en-us/privacypolicy.aspx> (last visited June 26, 2022). It created these policies, representations, and requirements, and publicly advertises them on its website as a means of increasing the value of its relationships with its members, thus allowing it to charge higher dues under the guise of enhanced security and information security practices.

20. SEIU 32BJ discloses certain situations and circumstances in which it uses and discloses PII. *Id.* None of the listed situations and circumstances describe the facts involved in the Data Breach.

21. Specifically, SEIU 32BJ discloses that it does collect information from website users and members:

What information we collect about you

We may collect personal information from and about our users, as well as information about users and their visits to the Websites. We do not knowingly collect any information from children under the age of 13.

Id.

22. Further, SEIU 32BJ discloses what information it may collect:

Personal Information:

When using certain areas of the Websites, you may be asked to provide or otherwise choose to provide personal information. We may collect personal information via the Websites through certain of users' activities, transactions, and completion of online forms on the Websites, for example, when users register for accounts or other features (such as our online courses or scholarships), complete surveys, submit a comment to one of our blogs, submit a question using an "ask us" or similar feature, send us an e-mail, submit information through the employer self-service system, or in any other way submit personal information to us via our Websites. *We consider "personal information" to include, for example, contact information (such as name, postal address, e-mail address and telephone number), social security number, date of birth, demographic information and other information that may identify you as an individual or allow contact with you as an individual.*

Id. (emphasis added).

23. Finally, SEIU 32BJ discusses the "commercially reasonable" efforts it takes to maintain the security of the information it collects:

Security

We use commercially reasonable security measures and take certain security measures to help protect against unauthorized access to or unauthorized alteration, disclosure, or destruction of data. These

measures include internal reviews of our data collection, storage, and processing practices and security measures, as well as physical security measures to guard against unauthorized access to systems where we store personal information.

While we endeavor to protect the security and integrity of the personal information provided by our users via the Websites, complete security is not always possible. Due to the inherent nature of the Internet as an open global communications vehicle, we cannot guarantee that information, during transmission through the Internet or while stored on our systems or otherwise in our care, will be absolutely safe from unauthorized access or use.

...

In the unlikely event that we believe that the security of any user's personal information in our possession or control may have been compromised, we may seek to notify such user of that development. If a notification is appropriate, we would endeavor to do so as promptly as possible under the circumstances, and, to the extent we have your e-mail address and if permitted under applicable laws, we may notify you by e-mail.

Id.

24. As a condition of membership and employment, SEIU 32BJ requires that individuals entrust it with highly confidential PII. As a result, SEIU 32BJ obtains, collects, and stores a massive amount of PII.

25. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, SEIU 32BJ assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff and Class Members' PII from disclosure.

26. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they rely on SEIU 32BJ to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

27. SEIU 32BJ was well aware that the PII it collects is highly sensitive and of significant value to those who would use it for wrongful purposes. As the Federal Trade Commission (FTC) recognizes, identity thieves can use this information to commit an array of crimes including identify theft, and fraud.¹ Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

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

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

30. The Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.² This time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used, compounds an identity theft victim’s ability to detect and address the harm.

31. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social

¹ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited June 30, 2022).

² *Identity Theft and Your Social Security Number*, Social Security Administrative, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed June 30, 2022).

Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

32. Further, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security Number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

33. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."³

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

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

³ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited June 30, 2022).

36. Despite all of the publicly available knowledge of the continued compromises of PII, SEIU 32BJ's approach to maintaining the privacy of the PII was lackadaisical, cavalier, reckless, or in the very least, negligent.

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

38. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.⁴

39. The delay in identifying and reporting the Data Breach caused additional harm to Plaintiff and Class Members. Plaintiff was not timely notified of the Data Breach, depriving him and the Class of the ability to promptly mitigate potential adverse resulting consequences.

40. As a result of a result of SEIU 32BJ's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at increased risk of suffering:

- a. Actual identity theft;
- b. Unauthorized use and misuse of their PII;
- c. The loss of the opportunity to control how their PII is used;
- d. The diminution in value of their PII;
- e. The compromise, publication, and/or theft of their PII;
- f. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

⁴ 2014 LexisNexis True Cost of Fraud Study, available at <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf> (last accessed June 30, 2022).

- g. Lost opportunity costs and lost wages associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;
- h. Costs associated with placing freezes on credit reports;
- i. Delay in receipt of tax refund monies or lost opportunity and benefits of electronically filing of income tax returns;
- j. The imminent and certain impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- k. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as it fails to undertake appropriate measures to protect the PII in its possession; and
- l. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

41. To date, SEIU 32BJ has not yet disclosed full details of the Data Breach. Without such disclosure, questions remain as to the full extent of the Data Breach, the actual data accessed and compromised, and what measures, if any, it has taken to secure the PII still in its possession. Through this litigation, Plaintiff seeks to determine the scope of the Data Breach and the information involved, obtain relief that redresses any harms, and ensure SEIU 32BJ has proper measures in place to prevent another breach from occurring in the future.

42. SEIU 32BJ was expressly prohibited by the Federal Trade Commission Act (“FTC Act”) (15 U.S.C. §45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The FTC has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

43. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.⁵

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.⁶ The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

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

46. SEIU 32BJ failed to properly implement basic data security practices. Its failure to employ reasonable and appropriate measures to protect against unauthorized access to PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

47. SEIU 32BJ was at all times fully aware of its obligation to protect PII and was also aware of the significant repercussions that would result from its failure to do so.

⁵ Federal Trade Commission, *Start With Security: A Guide for Business*, available at: <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last accessed June 30, 2022).

⁶ Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed June 30, 2022).

CLASS ACTION ALLEGATIONS

48. Plaintiff brings this action on behalf of himself and all others similarly situated pursuant to Rule 4:32-1 of the New Jersey Rules of Civil Procedure. This action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rule 4:32-1. The proposed Class is defined as:

All individuals whose PII was compromised in the SEIU 32BJ Data Breach.

Plaintiff Victor Mateo also brings his claims on behalf of a Subclass of New Jersey victims with subclass to be defined as follows:

All New Jersey current and former members of the union whose PII was compromised in the SEIU 32BJ Data Breach.

49. Excluded from the Class are Defendant, Defendant's subsidiaries and affiliates, its officers, directors, and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

50. Plaintiff reserves the right to modify or amend the definition of the proposed Class and Subclass and/or to add classes or subclasses, if necessary, before this Court determines whether certification is appropriate.

51. Numerosity: The Class Members are so numerous that joinder of all Members is impractical. The Class is comprised of over 200,000 individuals. Defendant has the administrative capability through its computer systems and other records to identify all members of the Class and Subclass, and such specific information is not otherwise available to Plaintiff.

52. Commonality: The questions here are ones of common or general interest such that there is a well-defined community of interest among the Members of the Class and Subclass. These questions predominate over questions that may affect only individual class members because SEIU 32BJ has acted on grounds generally applicable to the Class and Subclass. Such common legal or factual questions include, but are not limited to:

- a. Whether and to what extent Defendant had a duty to protect the PII of Class Members;
- b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;
- c. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;
- d. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;
- e. Whether Defendant failed to adequately safeguard the PII of Class Members;
- f. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- h. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- i. Whether Plaintiff and Class Members are entitled to actual, damages, statutory damages, and/or punitive damages as a result of Defendant's wrongful conduct;
- m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct;
- n. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach; and
- o. Whether Plaintiff and Class Members are entitled to additional identity theft protection.

53. Typicality: Plaintiff's claims are typical of the claims of the other members of the Class because Plaintiffs' PII, like that of every other Class Member, was not properly maintained or secured by Defendant. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Members of the Class were injured through the common misconduct of SEIU 32BJ. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

54. It is impracticable to bring the individual claims of the members of the Class and Subclass before the Court. Class treatment permits a large number of similarly situated persons or entities to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort, expense, or the possibility of inconsistent or contradictory judgments that numerous individual actions would engender. The benefits of the class mechanism, including providing injured persons or entities with a method for obtaining redress on claims that might not be practicable to pursue individually, substantially outweigh any difficulties that may arise in the management of this class action.

55. Adequacy of Representation: Plaintiff is a more than adequate representative of the Class in that Plaintiff's PII was compromised and has suffered damages. In addition:

- a. Plaintiff is committed to the vigorous prosecution of this action on behalf of himself and all others similarly situated and has retained competent counsel experienced in the prosecution of class actions and, in particular, class actions regarding data breaches;
- b. There is no conflict of interest between Plaintiff and the unnamed members of the Class or Subclass;
- c. Plaintiff anticipates no difficulty in the management of this litigation as a class action; and

- d. Plaintiff's legal counsel have the financial and legal resources to meet the substantial costs and legal issues associated with this type of litigation.

56. Plaintiff knows of no difficulty to be encountered in the maintenance of this action that would preclude its maintenance as a class action.

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

58. SEIU 32BJ has acted or refused to act on grounds generally applicable to the Class and Subclass, thereby making appropriate corresponding declaratory relief with respect to the Class and Subclass as a whole. SEIU 32BJ's actions and inactions challenged herein apply to and affect Class Members uniformly and hinges on its conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

59. Superiority of Class Action. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against a large organization like Defendant. Further, even for

those class members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

60. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

61. The litigation of the claims brought herein is manageable. SEIU 32BJ's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

62. Adequate notice can be given to Class Members directly using information maintained in SEIU 32BJ's records.

63. Unless a Class-wide injunction is issued, SEIU 32BJ may continue in its failure to properly secure the PII of Class Members, may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and may continue to act unlawfully as set forth in this Complaint.

64. All conditions precedent to bringing this action have been satisfied and/or waived.

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

65. Plaintiff and the Class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

66. Defendant had a duty to exercise reasonable care to protect and secure Plaintiff's and the Class Members' PII.

67. Through its acts and omissions, Defendant violated its duty to use reasonable care to protect and secure Plaintiff's and Class Members' PII as set forth herein and as follows:

- a. Defendant failed to physically or electronically protect and secure Plaintiff's and Class Members' PII;
- b. Defendant retained Plaintiff's and Class Members' PII longer than was reasonably necessary; and,
- c. Defendant failed to disclose the security breach in the most expedient time possible and without unreasonable delay to Plaintiff and Class Members.

68. Defendant breached the duties owed to Plaintiff and Class Members by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of information that resulted in the unauthorized access and compromise of PII; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; and (g) failing to follow its own privacy policies and practices.

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

70. Defendant's failure to adequately protect Plaintiff's and Class Members' PII was negligent.

71. Plaintiff's and Class Members' PII constitute personal property and due to Defendant's negligence their PII was exposed or stolen, resulting in harm to Plaintiff and Class Members.

72. Defendant's negligence directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' PII and Plaintiff and Class Members were (and continue to be) injured and have suffered (and will continue to suffer) the damages described herein.

73. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as SEIU 32BJ or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of SEIU 32BJ's duty.

74. SEIU 32BJ violated Section 5 of the FTCA by failing to use reasonable measures to protect PII and not complying with the industry standards. SEIU 32BJ's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a Data Breach.

75. Plaintiff and Members of the Class are consumers within the class of persons Section 5 of the FTCA was intended to protect.

76. SEIU 32BJ's violation of Section 5 of the FTCA constitutes negligence *per se*.

77. The harm that has occurred as a result of its conduct is the type of harm that the FTC Act was intended to guard against.

SECOND CAUSE OF ACTION

**Violation of the New Jersey Consumer Fraud Act, N.J.S.A. §§ 56:8 *et seq.*
(On Behalf of Plaintiff and the New Jersey Subclass)**

78. Plaintiff and the class re-allege and incorporate by reference each and every preceding paragraph of this Complaint.

79. The New Jersey Consumer Fraud Act defines merchandise as “any objects, wares, goods, commodities, services or anything offered, directly or indirectly to the public for sale.” N.J.S.A. § 56:8-1(c).

80. At all relevant times, Defendant SEIU 32BJ advertised and sold goods and services, including but not limited to membership in SEIU 32BJ, that are merchandise within the meaning of the New Jersey Consumer Fraud Act.

81. Under the New Jersey Consumer Fraud Act, the following qualifies as an unlawful practice:

The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby.

N.J.S.A. § 56:8-2.

82. In enacting the Identity Theft Prevention Act (ITPA), N.J.S.A. 56:8-161 to -166.3, which among other things, amended the New Jersey Consumer Fraud Act, the New Jersey Legislature found that “[i]dentity theft is an act that violates the privacy of our citizens and ruins

their good names: victims can suffer restricted access to credit and diminished employment opportunities, and may spend years repairing damage to credit histories.” N.J.S.A. § 56:11-45.

83. At all relevant times, SEIU 32BJ conducted business in New Jersey and collected PII from New Jersey residents within the meaning of the ITPA.

84. SEIU 32BJ violated the ITPA by failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay to: (i) customers, (ii) The New Jersey State Police, and (iii) Consumer Reporting Agencies, in violation of N.J.S.A. 56:8-163(a), N.J.S.A. 56:8-163(c)1, and N.J.S.A. 56:8-163(f).

85. Defendant’s failure to safeguard PII and its promises to do so constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation because Defendant knew that it had not adopted adequate electronic or physical safeguards to protect PII. More specifically, Plaintiff alleges that Defendant failed to implement and maintain reasonable security practices to protect PII, failed to store PII in a way that maximized its security and confidentiality, and permitted or failed to prevent the disclosure of PII.

86. Plaintiff and Class Members had a reasonable expectation that their PII would be protected and the failure to do so constitutes an unconscionable commercial practice, deception, fraud, false pretense, false promise, or misrepresentation in violation of N.J.S.A. § 56:8-2.

87. Defendant had a duty to advise Plaintiff and Class Members that its data security was inadequate, and by not doing so, concealed, suppressed, or omitted material facts.

88. Defendant intended for Plaintiff and the members of the proposed Class to rely upon the concealment, suppression, or omission of material fact relating to its data security.

89. Plaintiff and Class Members had a reasonable expectation that data security was adequate when they provided their PII to Defendant.

90. Plaintiff and Class Members would not have enrolled or renewed their memberships or provided their PII as required to Defendant if it had not concealed, suppressed, or omitted the material fact relating to its data security.

91. Defendant's actions constitute a knowing, concealment, suppression, or omission in violation of N.J.S.A. § 56:8-2. As a result of the foregoing, Plaintiff and Class Members suffered and will continue to suffer ascertainable losses and other damages as described in detail herein and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

92. Further, Defendant failed to dispose of stale records in violation of N.J.S.A. § 56:8-162, which requires that a business "destroy, or arrange for the destruction of, a customer's records within its custody or control containing personal information, which is no longer to be retained by the business or public entity, by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable, undecipherable or nonreconstructable through generally available means." N.J.S.A. § 56:8-162.

93. The New Jersey Consumer Fraud Act provides that it is "an unlawful practice and a violation of P.L. 1960, c. 39 (c. 56:8-1 et seq.) to willfully, knowingly or recklessly violate" Sections 56:8-161-164 of that Act.

94. In violation of N.J.S.A. § 56:8-162, Defendant retained its former members' PII well after such persons were no longer members of the union.

95. There are technologies available and programs that can be implemented that automatically wipe information when an event occurs ending the individual's relationship with the entity at issue. Because Defendant failed to employ any technologies to destroy the PII at issue, it has violated § 56:8-162 of the New Jersey Consumer Fraud Act.

96. As a result of the foregoing, Plaintiff and Class Members suffered and will continue to suffer ascertainable losses and other damages as described herein and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

97. In addition, Defendant failed to expediently notify victims following the Data Breach in violation of the New Jersey Consumer Fraud Act, N.J.S.A. 56:8-2 et seq.

98. Section 56:8-163 of the New Jersey consumer Fraud Act requires that a business conducting business in New Jersey:

shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

N.J.S.A. § 56:8-163.

99. The New Jersey Consumer Fraud Act defines a breach of security as follows:

“Breach of security” means unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the acquisition of personal information by an employee or agent of the business for a legitimate business purpose is not a breach of security, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

N.J.S.A. § 56:8-161. The Data Breach constituted a breach of security.

100. Defendant’s disclosure regarding the Data Breach to Plaintiff and Class Members was delayed and not made in the most expedient time possible.

101. As a result of the foregoing, Plaintiff and Class Members suffered and will continue to suffer ascertainable losses and other damages as described herein and are entitled to treble damages as provided by N.J.S.A. § 56:18-19.

102. Defendant's conduct as described above constituted a violation of the CFA, in that it failed to implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any PII collected or maintained by the business in the regular course of business, including information that identifies an individual.

THIRD CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

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

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

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

106. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of PII and remains at imminent risk that further compromises will occur in the future.

107. This Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure PII and to timely notify those affected of the Data Breach; and
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure PII.

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

109. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another breach at SEIU 32BJ occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified, and they will be forced to bring multiple lawsuits to rectify the same conduct.

110. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to SEIU 32BJ if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to SEIU 32BJ of complying with an injunction by employing reasonable prospective data security measures and communicating those measures to the Class is relatively minimal, and it has a pre-existing legal obligation to employ such measures.

111. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at SEIU 32BJ, thus eliminating the additional injuries that would result to Plaintiff and to those whose PII would be further compromised.

112. Plaintiff and the Class, therefore, seek a declaration (1) that SEIU 32BJ's existing security measures do not comply with their contractual obligations and duties of care to provide

adequate security, and (2) that to comply with their obligations and duties of care, SEIU 32BJ must implement and maintain reasonable security measures, including, but not limited to, the following:

- a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
- c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;
- d. Ordering that Defendant segment PII data by, among other things, creating firewalls and access controls so that if one area of Defendant's system is compromised, hackers cannot gain access to other portions of Defendant's systems;
- e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner all data not necessary for its provisions of services;
- f. Ordering that Defendant conduct regular computer system scanning and security checks;
- g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
- h. Ordering Defendant to meaningfully educate employees and members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

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

- A. For an order certifying the Class and Subclass and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;
- B. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- C. For compensatory, statutory, treble, and/or punitive damages in amounts to be determined by the trier of fact;

- D. For an order of restitution and all other forms of equitable monetary relief;
- E. Declaratory and injunctive relief as described herein;
- F. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;
- G. Awarding pre- and post-judgment interest on any amounts awarded; and
- H. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMANDED: A jury trial is demanded on all claims so triable.

Dated: July 28, 2022

Respectfully submitted,



Kenneth J. Grunfeld, Esq.
New Jersey Bar No. 026091999
Kevin W. Fay, Esq.
New Jersey Bar No. 005692010
GOLOMB SPIRT GRUNFELD, P.C.
1835 Market Street
Suite 2900
Philadelphia, PA 19103
Telephone: (215) 985-9177
kgrunfeld@golomblegal.com
kfay@golomblegal.com

Designated as Trial Counsel

CERTIFICATION OF COMPLIANCE WITH RULE 1:38-7(C)

I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with Rule 1:38-7(b).

Dated: July 28, 2022

GOLOMB SPIRT GRUNFELD, P.C.

A handwritten signature in black ink, appearing to read 'Ken Grunfeld', written in a cursive style.


KENNETH J. GRUNFELD, ESQUIRE

CERTIFICATION OF NO OTHER ACTIONS

I certify that the dispute about which I am suing is not the subject of any other action pending in any other court or a pending arbitration proceeding to the best of my knowledge and belief. Also, to the best of my knowledge and belief no other action or arbitration proceeding is contemplated. Further, other than the parties set forth in this complaint, I know of no other parties that should be made a part of this lawsuit. In addition, I recognize my continuing obligation to file and serve on all parties and the court an amended certification if there is a change in the facts stated in this original certification.

Dated: July 28, 2022

GOLOMB SPIRT GRUNFELD, P.C.

A handwritten signature in black ink, appearing to read 'Ken Grunfeld', with a long horizontal flourish extending to the right.

KENNETH J. GRUNFELD, ESQUIRE

EXHIBIT 1



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336



400554040000473379
000 0007069 00000000 0001 0004 01768 INS: 0 0

VICTOR MATEO
130 ORIENT WAY
APT 2L
RUTHERFORD NJ 07070-2163

February 11, 2022

NOTICE OF SECURITY INCIDENT/DATA BREACH

Dear Victor Mateo:

Service Employees International Union, Local 32BJ, ("32BJ") writes to make you aware of a recent incident that may impact the privacy of some of your information. You are receiving this letter because you are potentially impacted by this incident. 32BJ is providing you with notice of the incident, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

What Happened? On November 1, 2021, 32BJ experienced a data security incident that impacted a limited number of 32BJ computer systems. We immediately responded and launched an investigation with cybersecurity experts to confirm the nature and scope of the incident and determine the impact to 32BJ data. Through the investigation, we learned that an unauthorized actor accessed certain files and folders within the 32BJ system and may have viewed or acquired data containing certain member information between October 21, 2021 until November 1, 2021.

We conducted a thorough programmatic and manual review of the potentially impacted files and folders to determine whether they contained any sensitive data. We recently concluded our review and determined on or around January 13, 2022, that information related to you was included in the potentially impacted files. After determining the scope of information in the impacted files, we undertook efforts to locate address information for the affected individuals, put resources in place, and provide this direct notice.

What Information Was Involved? The information present in the files that may have been viewed or acquired as a result of this incident included your name, and date of birth; Social Security number.

What We Are Doing. We treat our responsibility to safeguard the information entrusted to us as an utmost priority. As such, we responded immediately to this incident and have been working diligently to provide you with an accurate and complete notice of the incident. Our immediate response to this event also included prompt and continued correspondence with federal law enforcement authorities. As part of our ongoing commitment to the privacy and security of information in our care, we are reviewing our existing policies and procedures relating to data protection and security and implemented enhanced security controls on our remote access system. We also changed system passwords and upgraded our security tools. We will continue to evaluate additional security measures to mitigate any potential risk associated with this incident and to better prevent similar incidents in the future.

As an added precaution, we are providing you with 12 months of complimentary access to credit monitoring and identity restoration services through Equifax, as well as guidance on how to better protect your information. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. You can find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*. There, you will find additional information about the complimentary credit monitoring and identity restoration services we are offering and how to enroll.



Civil Case Information Statement

Case Details: BERGEN | Civil Part Docket# L-004121-22

Case Caption: MATEO VICTOR VS SEIU

Case Initiation Date: 07/28/2022

Attorney Name: KENNETH JAY GRUNFELD

Firm Name: GOLOMB SPIRT GRUNFELD, PC

Address: 1835 MARKET ST STE 2900

PHILADELPHIA PA 19103

Phone: 2159859177

Name of Party: PLAINTIFF : Mateo, Victor

Name of Defendant's Primary Insurance Company
(if known): Unknown

Case Type: COMPLEX COMMERCIAL

Document Type: Complaint with Jury Demand

Jury Demand: YES - 12 JURORS

Is this a professional malpractice case? NO

Related cases pending: NO

If yes, list docket numbers:

Do you anticipate adding any parties (arising out of same transaction or occurrence)? NO

Does this case involve claims related to COVID-19? NO

Are sexual abuse claims alleged by: Victor Mateo? NO

THE INFORMATION PROVIDED ON THIS FORM CANNOT BE INTRODUCED INTO EVIDENCE

CASE CHARACTERISTICS FOR PURPOSES OF DETERMINING IF CASE IS APPROPRIATE FOR MEDIATION

Do parties have a current, past, or recurrent relationship? YES

If yes, is that relationship: Other(explain) Union/Union Member

Does the statute governing this case provide for payment of fees by the losing party? NO

Use this space to alert the court to any special case characteristics that may warrant individual management or accelerated disposition:

Putative class action regarding a data breach

Do you or your client need any disability accommodations? NO

If yes, please identify the requested accommodation:

Will an interpreter be needed? NO

If yes, for what language:

Please check off each applicable category: Putative Class Action? YES Title 59? NO Consumer Fraud? NO

I certify that confidential personal identifiers have been redacted from documents now submitted to the court, and will be redacted from all documents submitted in the future in accordance with *Rule* 1:38-7(b)

07/28/2022
Dated

/s/ KENNETH JAY GRUNFELD
Signed

