IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF PENNSYLVANIA

LISA CHAPMAN,
individually and on behalf of
a class of similarly situated individuals
New Kensington, PA

Plaintiff,

v.

COMMONWEALTH OF
PENNSYLVANIA
DEPARTMENT OF HEALTH
8th Floor West
625 Forster Street
Harrisburg, PA 17120

and

INSIGHT GLOBAL, INC
4170 Ashwood Dunwoody Road
Atlanta, GA 30319

Defendants.

Civil Case No.:

COMPLAINT—CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Lisa Chapman ("Plaintiff"), individually and on behalf of the Classes defined below of similarly situated persons, brings this Class Action Complaint and alleges the following against Defendants, the Pennsylvania Department of Health ("DOH") and Insight Global, Inc. ("Insight"), based upon personal knowledge with respect to Plaintiff and upon 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 class action arises out of the recent cyberattack and data breach involving Insight and the DOH (the "Data Breach"), which collected and stored certain private health information ("PHI") of the Plaintiff, and the putative Class Members, all of whom have PHI on Insight and DOH servers.

2. The PHI compromised in the Data Breach included highly-sensitive information including but not limited to name, gender, phone number, sexual orientation, family size, and health data.

3. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' PHI.

4. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' PHI that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

PARTIES

5. Plaintiff is an adult individual and citizen of the Commonwealth of Pennsylvania who resides in New Kensington, Westmoreland County, Pennsylvania..

6. Defendant DOH is a government entity with a primary, principal place of business address of 8th Floor West, 625 Forster Street, Harrisburg, Dauphin County, Pennsylvania, 17120.

7. Defendant Insight is an employment staffing company with its principal place of business and headquarters at 4170 Ashford Dunwoody Road, Atlanta, Georgia 30319. Insight conducts business throughout Pennsylvania.

8. At all times relevant hereto, Plaintiff was a citizen of the Commonwealth of Pennsylvania whose PHI was disclosed without authorization to unknown third parties as a result of the data disclosure described above.

JURISDICTION AND VENUE

9. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' states of citizenship.

10. This court has personal jurisdiction over Defendant DOH because its principal place of business, headquarters and sole operational domain is within this District.

11. This court has personal jurisdiction over Defendant Insight because it is authorized to and does conduct substantial business in this District.

12. Venue is proper under 28 U.S.C. §1391(b) because the cause of action upon which the complaint is based arose throughout the Commonwealth of Pennsylvania, including in Dauphin County, which is in the Middle District of Pennsylvania.

COMMON FACTUAL ALLEGATIONS

13. Plaintiff and the proposed Class are individuals who were either diagnosed with or in close proximity to individuals diagnosed with COVID-19, and who were contacted by Insight on behalf of DOH for the purposes of contact tracing to understand, address, and potentially slow the spread of COVID-19.

14. "Contact tracing" is the process of notifying individuals of exposure to COVID-19, addressing questions and concerns, referring for testing, encouraging self-quarantine, monitoring of symptoms, and assessing the need for additional supportive services during the quarantine period.[1]

15. Plaintiff brings this class action against Defendants for Defendants' failure to properly secure and safeguard protected health information as defined by the Health Insurance Information Portability and Accountability Act ("HIPAA"), medical information, and other personally identifiable information, for failing to comply with industry standards to protect and safeguard that information, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other members of the class that such information had been compromised.

16. Insight is an employment staffing company headquartered in Atlanta, Georgia, which does business throughout Pennsylvania.

17. DOH is a government entity of the Commonwealth of Pennsylvania.

18. Insight was contracted by DOH to perform contact tracing analysis and other services beginning in 2020.

19. There was no competitive bidding process for the contract, which totaled approximately $23 million, between Insight and DOH.

[1] https://www.cdc.gov/coronavirus/2019-ncov/global-covid-19/operational-considerations-contact-tracing.html (last accessed May 4, 2021).

20. DOH at all times relevant hereto asserted that "all communication related to contact tracing is private and confidential" and that "your information will stay confidential."[2]

21. Over a period of months in 2020 and 2021, employees of Insight contacted residents of the Commonwealth of Pennsylvania including Plaintiff and the proposed Class and obtained sensitive and protected health information including but not limited to name, gender, phone number, sexual orientation, gender presentation, family size, and health data (hereinafter, collectively, "PHI").

22. Insight failed to secure the PHI of the individuals it contacted.

23. Insight maintained unsecure spreadsheets, databases, and or/documents containing the PHI of tens of thousands of Class Members.

24. These documents were widely available to the public through a Google search and did not require a password, log in, or any kind of authentication in order to be viewed.

25. Insight was aware that its employees were using unsecure data storage and communications methods as early as November 2020. *See* Exhibit A, emails exchanged between employees of Insight.

[2] https://www.health.pa.gov/topics/disease/coronavirus/Pages/Contact-Tracing.aspx (last accessed May 4, 2021).

26. DOH was notified of this breach as early as February 2021. *See* Exhibit B, an email from a former employee of Defendant Insight to the Pennsylvania Department of Health Office of Legal Counsel.

27. Neither DOH nor Insight took any action to secure the PHI of Plaintiff or other class members until at least April 21, 2021. *See* "Notice of Data Event Related to Pennsylvania Contact Tracing" at Exhibit C (printed from Insight's website on May 5, 2021).

28. Neither DOH nor Insight took any action to notify Plaintiff or other class members of this breach until at least April 29, 2021. *See* Exhibit C.

29. DOH obtained COVID-19 test results for all persons who tested positive for the disease via the PA National Electronic Disease Surveillance System ("PA-NEDSS"), a system which "facilitates electronically transferring public health surveillance data from the healthcare system to public health departments."[3]

30. At all times relevant hereto, DOH was a covered entity under the terms of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and asserted that it keeps the health information of Pennsylvanians

[3] https://www.health.pa.gov/topics/Reporting-Registries/Pages/PA-NEDSS.aspx (last accessed May 4, 2021).

private. *See* Exhibit D, "Commonwealth of Pennsylvania Department of Health (DOH) Notice of Privacy Practices for Protected Health Information."

31. Insight is a business associate of DOH under the terms of HIPAA.

32. As a business associate of DOH, Insight was required to "establish and maintain appropriate safeguards to prevent any use or disclosure of PHI." *See* Exhibit E, "Commonwealth of Pennsylvania Business Associate Appendix – HIPAA Compliance."

33. Defendants have acknowledged the sensitive and confidential nature of the information here at issue. Defendants have acknowledged through conduct and statements that the misuse or inadvertent disclosure of PHI can pose significant financial and privacy risks, and that they may not disclose and must take reasonable steps to protect such PHI from improper release and disclosure.

34. Despite these acknowledgements and averments that all PHI obtained in connection with COVID-19 contact tracing would be kept private and confidential, Defendants failed to take appropriate or even the most basic steps to protect the PHI of Plaintiff and other class members from being disclosed.

35. As a result of Defendants' failure to implement and follow even the most basic security procedures, Plaintiff's and other class members' PHI is now in the hands of the general public including thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other class

members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendants' Data Breach.

36. Plaintiff and other class members have had their most personal, sensitive and private information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

37. Plaintiffs bring this class action against Defendants for Defendants' failure to properly secure and safeguard PHI and for failing to provide timely, accurate, and adequate notice to Plaintiff and other class members that their PHI had been compromised.

38. For the reasons mentioned above, DOH's and Insight's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class significant injuries and harm in several ways. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social

engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

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

40. As a result of the DOH and Insight's failures, Plaintiff and Class members are at substantial risk of suffering identity theft and fraud or misuse of their PHI.

41. Plaintiff and Class members are also at a continued risk because their information remains in the DOH's and Insight's systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as the DOH and Insight fail to undertake the necessary and appropriate security and training measures to protect individuals' PHI.

42. Plaintiff, individually and on behalf of all other similarly situated individuals alleges claims in negligence, negligence per se, and publicity given to private life.

CLASS ACTION ALLEGATIONS

43. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure.

44. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons in the United States whose PHI was compromised in the Data Breach disclosed by DOH and Insight between March 16, 2020 and April 29, 2021 (the "Nationwide Class").

45. Plaintiff proposes the following Subclass definition, subject to amendment as appropriate:

> All persons in the Commonwealth of Pennsylvania whose PHI was compromised in the Data Breach disclosed by DOH and Insight between March 16, 2020 and April 29, 2021 (the "Pennsylvania Subclass").

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

47. Plaintiff hereby reserves the right to amend or modify the class

definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Classes meet the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

48. Numerosity. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Classes consists of at least thousands of people whose data was compromised in the Data Breach.

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

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PHI;

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

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendants owed a duty to Class Members to safeguard their PHI;

f. Whether Defendants breached its duty to Class Members to safeguard their PHI;

g. Whether computer hackers obtained Class Members' PHI in the Data Breach;

h. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendants' conduct was negligent;

j. Whether Defendants' conduct constitutes negligence *per se*;

k. Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendants violated the Federal Trade Commission Act ("FTC Act");

m. Whether Defendants violated the Health Insurance Portability and Accountability Act ("HIPAA");

n. Whether Defendants violated Pennsylvania's Policies and Procedures for Medical Records Services, 28 Pa. Code § 115.1, *et. seq.*;

o. Whether Defendants were unjustly enriched to the detriment of Plaintiff and the Class;

p. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and

q. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

50. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class Member, was compromised in the Data Breach.

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

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

53. Superiority. A class action is superior to other available methods for

the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

55. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and the Classes to exercise due care in collecting, storing, using, and safeguarding their PHI;

b. Whether Defendants' data security practices were reasonable in light of best practices recommended by data security experts;

c. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence *per se*;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PHI; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

//

//

//

//

CAUSES OF ACTION

FIRST COUNT

Negligence
(On Behalf of Plaintiff individually and on Behalf of the Nationwide Class and/or Pennsylvania Subclass)

57. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

58. By accepting Plaintiff's and other class members' non-public personal information, Defendants DOH and Insight assumed a duty to use reasonable and, at the very least, industry standard care to secure such information against disclosure, theft, and misuse.

59. Defendants DOH and Insight breached their duty of care in failing to adequately, or in any meaningful way, secure and protect the PHI of Plaintiff and other class members from disclosure, theft, and misuse.

60. Defendants DOH and Insight further breached their duty of care by failing to promptly, clearly, and accurately inform Plaintiff and other class members that their personal information had been disclosed.

61. Plaintiff and other members of the class have suffered injury in fact including monetary damages and will continue to be injured and incur damages as a result of Defendants' negligence and misconduct.

62. As a direct and proximate result of the negligence of Defendants DOH and Insight in failing to take adequate steps to protect the personal information in their care, Plaintiff and other members of the class now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Defendants' failures.

63. As a direct and proximate result of the negligence of Defendants DOH and Insight in failing to take adequate steps to protect the personal information in their care, Plaintiff and other class members have had their most personal and private information disseminated to the public at large and now expenrenience and will continue to experience emotional pain and mental anguish and embarrassment.

64. The publicly accessible posting of Plaintiff and other class members' PHI combined with the complete and total lack of any security measures whatsoever including but not limited to a log in requirement, password protection, or encryption evidences a reckless and wanton disregard for the private information of Plaintiff and other class members which entitles them to punitive damages.

65. As a direct and proximate result of the DOH and Insight's negligence, Plaintiff and the Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

SECOND COUNT

Negligence *Per Se*

(On Behalf of Plaintiff individually and on Behalf of the Nationwide Class and/or Pennsylvania Subclass)

66. Plaintiff restates and realleges all proceeding factual allegations above as if fully set forth herein.

67. 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 entities such as the DOH and Insight for failing to use reasonable measures to protect PHI. Various FTC publications and orders also form the basis of the DOH's and Insight's duty.

68. The DOH and Insight violated Section 5 of the FTC Act by failing to use reasonable measures to protect PHI and not complying with the industry standard. The DOH's and Insight's conduct was particularly unreasonable given the nature and amount of PHI it obtained and stored and the foreseeable consequences of a data breach involving PHI of the individuals they contacted.

69. The DOH's and Insight's violation of Section 5 of the FTC Act constitutes negligence *per se*.

70. Plaintiff and members of the Class are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

71. The DOH and Insight is an entity covered under the Health Insurance Portability and Accountability Act ("HIPAA") which sets minimum federal standards for privacy and security of PHI.

72. Pursuant to HIPAA, 42 U.S.C. § 1302d, *et. seq.*, and its implementing regulations, DOH and Insight had a duty to implement and maintain reasonable and appropriate administrative, technical, and physical safeguard to protect Plaintiff's and the Class members' electronic PHI.

73. Specifically, HIPAA required the DOH and Insight to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq.*

74. HIPAA also requires the DOH and Insight to provide Plaintiff and the Class members with notice of any breach of their individually identifiable PHI "without unreasonably delay and in no case later than 60 calendar days after discovery of the breach." 45 CFR §§ 164.400-414.

75. The DOH and Insight violated HIPAA by actively disclosing Plaintiff's and the Class Members' electronic PHI; by failing to provide fair,

reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PHI; and by failing to provide Plaintiff and Class members with notification of the Data Breach within 60 days after its discovery.

76. Plaintiff and the Class members are individuals within the class of persons HIPAA was intended to protect.

77. The DOH and Insight's violation of HIPAA constitutes negligence *per se*.

78. Pursuant to Pennsylvania's Policies and Procedures for Medical Records Services, 28 Pa. Code § 115.1, *et. seq.* (the "Pa. Policies"), the DOH and Insight were required to have a medical record service "properly equipped to enable its personnel to function in an effective manger and to maintain medical records so that they are readily accessible and secure from unauthorized use."

79. They were also required to train its medical record service personnel. *Id*.

80. Additionally, the DOH and Insight were required to store medical records "in such a manner as to provide protection from loss, damage and unauthorized access." *Id*.

81. Pursuant to the Pa. Policies, the DOH was required to treat "all records" (including those of Plaintiff's and the Class members) "as confidential." *Id*.

82. The DOH and insight violated the Pa. Policies by actively disclosing Plaintiff's and the Class members' PHI; by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PHI; and failing to maintain the confidentiality of Plaintiff's and the Class members' records.

83. Plaintiff and the Class members are individuals within the class of persons the Pa. Policies was intended to protect.

84. The DOH and Insight's violation of the Pa. Policies constitutes negligence *per se.*

85. The harm that has occurred as a result of the DOH and Insight's conduct is the type of harm that the FTC Act, HIPAA, and/or the Pa. Policies was intended to guard against.

86. As a direct and proximate result of the DOH and Insight's negligence, Plaintiff and the Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

//

//

//

THIRD COUNT

Publicity Given to Private Life

(On Behalf of Plaintiff individually and on Behalf of the Nationwide Class and/or Pennsylvania Subclass)

87. Plaintiff re-alleges and incorporates by reference all preceding allegations as if fully set forth herein.

88. As alleged herein, from 2020 through 2021, Defendants caused the PHI of Plaintiff and other members of the class to be widely, openly, and generally available to the public despite their duty to keep this information private and confidential.

89. Specifically, Defendants disseminated or caused to be disseminated the Plaintiff's private and protected information including but not limited to her COVID-19 status.

90. Such information is private information, the disclosure of which would be highly offensive to a reasonable person and which is not of legitimate concern to the public.

91. Plaintiff believes and therefore avers that the disclosure of her private information shows reckless and wanton disregard for her privacy which entitles Plaintiff to punitive damages.

92. As a direct and proximate result of the DOH and Insight's disclosure of Plaintiff and Class Members' PHI, Plaintiff and the Class Members have been

injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Classes, prays for judgment as follows:

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

b. For equitable relief enjoining DOH and Insight from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PHI;

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

d. For an order requiring Defendants to pay for not less than seven years of credit monitoring services for Plaintiff and the Class(es);

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: May 5, 2021

Respectfully Submitted By:

SHUB LAW FIRM LLC

/s/ Jonathan Shub
Jonathan Shub, Esquire
PA Attorney I.D. #53965
Kevin Laukaitis, Esquire
PA Attorney I.D. #321670
134 Kings Highway East, 2nd Floor
Haddonfield, NJ 08033
(856) 772-7200
jshub@shublawyers.com
klaukaitis@shublawyers.com

SCHMIDT KRAMER, P.C.
SCOTT B. COOPER, Esquire
PA Attorney I.D. #70242
209 State Street
Harrisburg, PA 17101
(717) 232-6300
scooper@schmidtkramer.com

HAGGERTY, GOLDBERG, SCHLEIFER & KUPERSMITH, P.C.

JAMES C. HAGGERTY, Esquire
PA Attorney I.D. # 30003
1835 Market Street, Suite 2700
Philadelphia, PA 19103
(267) 350-6600
jhaggerty@hgsklawyers.com

JACK GOODRICH & ASSOCIATES, PC

JOHN P. GOODRICH, Esquire
PA Attorney I.D. #49648
To be admitted pro hac vice
Lauren R. Nichols, Esquire
PA Attorney I.D. #313520
To be admitted pro hac vice
429 Fourth Avenue, Suite 900
Pittsburgh, PA 15219
(412) 261-4663
jack@goodrichpc.com
lauren@goodrichpc.com

PHIL DILUCENTE & ASSOCIATES, LLC

PHILIP P. DILUCENTE, ESQUIRE
PA Attorney I.D. #87295

To be admitted pro hac vice
Kenneth Nolan, Esquire
PA Attorney ID #32422
To be admitted pro hac vice
310 Grant Street, Suite 1801
Pittsburgh, PA 15219
412-281-5005
phil@getphil.com
ken@getphil.com

Attorneys for Plaintiff and the Proposed Classes

ClassAction.org