UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

ANDREW GIANCOLA, RAYMOND T. SCOTT, and PATRICIA SMITH, Individually and On Behalf of All Others Similarly Situated, Plaintiffs, v. LINCARE HOLDINGS, INC., Defendant.	Case No.: **CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

INTRODUCTION

By and through their undersigned counsel, Plaintiffs Andrew Giancola, Raymond T. Scott, and Patricia Smith ("Plaintiffs") bring this class action against Defendant Lincare Holdings, Inc. ("Defendant" or "Lincare"), on behalf of themselves and a class of similarly situated persons (the "Class" or "Class Members"). Plaintiffs allege the following based upon personal knowledge, or where there is no personal knowledge, upon the investigation of their counsel and/or upon information and belief.

NATURE AND SUMMARY OF THE ACTION

1. This class action arises from Lincare's voluntary failure to adequately safeguard and protect the highly confidential and sensitive, personally-identifiable information ("PII"), including social security and W-2 information, of its own current and former employees. Plaintiffs, on behalf of themselves and other current and former Lincare employees who had their PII wrongfully and voluntarily disseminated by Defendant to a third-party or parties, seek to recover for the substantial damages that have been caused, and will continue to be caused, by Defendant's flagrant violations of their rights, and the insufficient remedy afforded by Defendant.

2. Lincare is a home-healthcare company based in Florida. Lincare is one of the largest suppliers of home respiratory-therapy products and services in the United States, employing over 14,000 employees nationwide in over 1,000 locations.

3. On February 3, 2017, a Lincare Human Resources ("HR") employee disseminated and disclosed unencrypted PII—including the names, addresses, social security numbers, earnings information, and other highly sensitive information—of current and

former Lincare employees to a third-party who requested such information via an e-mail purporting to be from a Lincare senior-level executive (the "Data Breach"). The Lincare employee did not bother to confirm or authenticate the validity of the request prior to sending the highly sensitive and confidential PII of Plaintiffs and the Class Members to the third-party. Indeed, despite being placed on ample notice of the risks of such data breaches, Lincare failed to implement the most basic security precautions or checks before releasing its own employees' PII.

4. Social security numbers and salary information are entitled to a particularly high level of protection due to their sensitive and confidential nature. The combination of this information with other identifying information, such as the names and addresses of employees, enhanced the sensitivity of the information made susceptible to abuse and exploitation, and required the utmost protection in its handling. Lincare knew and understood the confidential and private nature of Plaintiffs' and the Class Members' PII, and owed duties to Plaintiffs and the Class Members to protect and maintain the confidentiality of their PII. In particular, social security numbers are perhaps the most important piece of information to an individual, and are not easily replaced. Unlawful exploitation of social security numbers costs the federal government hundreds of millions of dollars each year from the fraudulent filing of tax returns by identity thieves, not to mention the harms suffered by persons whose social security numbers are stolen and/or misappropriated.

5. It is well-known, and the subject of many media reports, that PII data is highly coveted by, and the frequent target of, hackers and cybercriminals. Legitimate organizations and the criminal underground alike recognize the value in PII. Otherwise, they wouldn't pay

for it or aggressively seek it. PII data has been stolen and sold by the criminal underground on many occasions in the past, and the accounts of the thefts and unauthorized access have been the subject of many media reports. In recent years, criminals have increasingly been drawn to unlawfully obtaining PII because they can use biographical data from multiple sources to perpetuate more and larger thefts.[1] Illicitly obtained PII, sometimes aggregated from different breaches, is sold on the black market, including on websites.[2] In turn, identity thieves can use PII, *inter alia*, to open new financial accounts and incur charges in another person's name, take out loans in another person's name, incur charges on existing accounts, clone ATM, debit, or credit cards, obtain a job or housing, and commit various types of government crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, and filing a fraudulent tax return using the victim's information to obtain a fraudulent refund. Worse yet, some of this activity may not come to light for years, and may continue in perpetuity.

6. Due to Lincare's failure to implement the most basic of safeguards and precautions, the most sensitive data of Lincare's current and former employees, including social security numbers, W-2 information, and other PII, is now in the possession of an unknown third-party or parties who have already used the PII for illegal purposes, and will be able to continue doing so indefinitely. This unauthorized third-party or parties gained access

[1] *See* Verizon 2014 PCI Compliance Report, Verizon, http://www.verizonenterprise.com /resources/reports/rp_pci-report-2014_en_xg.pdf (last visited Oct. 5, 2017).

[2] *See, e.g.*, *How Much Is Your Identity Worth?*, Krebs on Security, http://krebsonsecurity.com /2011/11/how-much-is-your-identity-worth/ (last visited Oct. 5, 2017).

to the PII of Plaintiffs and the Class Members for the purpose of using the information for improper and unlawful purposes, including identity theft, the filing of false tax returns, and the submission of fraudulent student loan applications and fraudulent credit applications.

7. As a direct and proximate result of Lincare's failure to maintain adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect the PII of its employees—and despite numerous, repeated warnings from the Internal Revenue Service ("IRS") and Federal Bureau of Investigation ("FBI") regarding the imminent risks of this precise issue, the well-publicized data breaches that have occurred recently nationwide, and Lincare's own recent Health Insurance Portability and Accountability Act of 1996 ("HIPAA") violation involving failure to safeguard records containing patients' personal health information—Plaintiffs and the Class Members have had their PII compromised and have suffered substantial harm from the misuse of their PII. Plaintiffs and the Class Members have been placed at risk of current and future fraud, identity theft, and financial injury, and have incurred direct and significant financial and temporal expenses that they will continue to incur in the future, including, *inter alia*, costs associated with credit and identity theft monitoring, protection, and repair, replacement and repair of compromised financial information, and other measures needed to protect against and resolve the misuse of their PII.

8. Based on the misconduct alleged herein, Plaintiffs allege claims against Defendant for negligence, breach of fiduciary duty, breach of implied contract, violation of the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), and declaratory

judgment. Plaintiffs seek on behalf of themselves and all Class Members monetary damages, restitution, injunctive relief, and all other relief deemed appropriate.

JURISDICTION AND VENUE

9. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and members of the proposed Class are citizens of different states than Defendant Lincare. Lincare is a for-profit business entity incorporated in Delaware, with its principal place of business and corporate headquarters located in Clearwater, Florida.

10. This Court has personal jurisdiction over Lincare because Lincare maintains its headquarters in Florida, is registered to conduct, and does in fact conduct, substantial business in Florida, and has sufficient minimum contacts with Florida.

11. Venue is proper in this District under 28 U.S.C. § 1391(b) because Lincare resides in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

THE PARTIES

A. Plaintiffs

12. Plaintiff Andrew Giancola is a resident of Florida. Giancola is a former employee of Lincare, having served in various positions—including financial analyst, financial analyst manager, and contract manager—for nearly four and a half years, from September 2012 until March 1, 2017. As a Lincare employee, Giancola was required to, and

did in fact, provide his PII, including his social security number and W-2 tax information, to Lincare, which information was disseminated and compromised in the Data Breach.

13. Plaintiff Raymond T. Scott is a resident of Florida. Scott is a former employee of Lincare, having served in various positions—including safety administrator, facilities manager, and safety analyst—for nearly eight years, from April 2008 until February 2016. As a Lincare employee, Scott was required to, and did in fact, provide his PII, including his social security number and W-2 tax information, to Lincare, which information was disseminated and compromised in the Data Breach. Scott was also required to, and did in fact, provide the PII of his spouse in order to obtain certain employment-related benefits through Lincare.

14. Plaintiff Patricia Smith is a resident of Florida. Smith is a former employee of Lincare, having served in various positions—including garnishment specialist and payroll specialist—for nearly 11 years, from October 2000 to September 2006, and then from May 2011 until October 2016. As a Lincare employee, Smith was required to, and did in fact, provide her PII, including her social security number and W-2 tax information, to Lincare, which information was disseminated and compromised in the Data Breach.

15. Each Plaintiff had their PII compromised due to the Data Breach, and has been injured as a result.

B. Defendant

16. Lincare is a corporation organized under the laws of Delaware, with its principal place of business in Clearwater, Florida.

FACTUAL ALLEGATIONS

A. Background on PII and Data Breaches

17. A person's social security number is perhaps the most important piece of information to an individual in the modern world. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a social security number "your secret sauce," that is "as good as your DNA to hackers."[3] Social security numbers are used, among other things, to verify eligibility for employment, to apply for a passport, to open a bank account, or to apply for a credit card, student loan, or mortgage. A social security number is also needed to obtain government benefits like social security and Medicare. Social security numbers are assigned to citizens (and sometimes to noncitizens) as early as their birth, and are required to enroll in school and to obtain healthcare services. A social security number follows a person through life.

18. The United States Government Accountability Office ("GAO") noted as far back as June 2007, in a report on data breaches ("GAO Report"), that identity thieves use identifying data such as social security numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[4] As the GAO Report states, this type of identity theft is the most harmful because it may take some time for the victim to become aware of the theft, and can adversely impact the victim's credit rating. In

[3] *See* Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, KIPLINGER, http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited Oct. 5, 2017).

[4] *See Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, United States Government Accountability Office, http://www.gao.gov/new.items/d07737.pdf (last visited Oct. 5, 2017).

addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."

19. According to the Federal Trade Commission ("FTC"), identity-theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[5] Identity thieves use stolen, personal information such as social security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[6]

20. Identity-theft crimes often include more than just crimes of financial loss. Identity thieves can also commit various types of government fraud, such as obtaining a driver's license or official identification card in the victim's name but with the thief's picture, using the victim's name and social security number to obtain government benefits, and/or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's social security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[7] Further,

[5] *See generally Identity Theft Consumer Information*, Federal Trade Commission, https://www.ftc.gov/idtheft (last visited October 5, 2017); Federal Trade Commission, *Identity Theft Recovery*, https://www.identitytheft.gov (last visited October 5, 2017).

[6] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*

[7] *See* FTC Identity Theft Website, *supra*.

loss of private and personal health-information can expose the victim to loss of reputation, loss of job employment, blackmail, and other negative effects.[8]

21. The theft of social security numbers in particular, as opposed to other PII, is difficult to rectify because a person whose personal information has been compromised may not see any signs of identity theft for years, social security numbers are difficult to change, and their misuse can continue for years into the future. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the 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.

22. Sensitive information, such as social security numbers, is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for a number of years.[9] As a result

[8] *See Identity Smart: A Guide For Consumers to Help Protect Against Identity Theft*, The National Crime Prevention Council, http://www.ncpc.org/resources/files/pdf/theft/NCPC-ID%20Theft.pdf (last visited Oct. 5, 2017) (stating that identity thieves "may threaten national security or commit acts of terrorism" and noting that the September 11 hijackers used fake ID's to board their planes); *see also* Bob Sullivan, *9/11 report light on ID theft issues*, NBC NEWS, http://www.nbcnews.com/id/5594385 (last visited Oct. 5, 2017) (stating that the September 11 hijackers "liberally used document fraud prior to that date, some to ease entrance into the United States, others to move around once they were here and to obtain drivers' licenses they needed to board the airplanes").

[9] Companies, in fact, also recognize Sensitive Information as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market. *See Every Click Matters*, Norton by Symantec, https://community.norton.com /en/blogs/symantec-cyber-education/every-click-matters (last visited October 5, 2017); *see also* T. Soma, *et al.*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–*4 (2009).

of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, social security numbers, and other sensitive information directly on various, internet websites making the information publicly available. In one study, researchers found hundreds of websites displaying stolen, sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism—the "Safe Browsing list." The study concluded:

> It is clear from the current state of the credit card black-market that cyber criminals can operate much too easily on the Internet. They are not afraid to put out their email addresses, in some cases phone numbers and other credentials in their advertisements. It seems that the black market for cyber criminals is not underground at all. In fact, it's very "in your face."[10]

23. A similar, recent report about healthcare-related identity-theft fraud, sponsored by Experian, indicated that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000."[11] Moreover, a majority of the victims were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage. Almost fifty (50) percent of the victims lost their healthcare coverage as a result of the incident, while nearly one-third said their insurance premiums went up after the event. Forty (40) percent of the consumers were never able to resolve their identity theft at all. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.[12]

---

[10] *See The "Underground" Credit Card Blackmarket*, Stop The Hacker, http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited Oct. 5, 2017).

[11] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, http://news.cnet.com/8301-27080_3-10460902-245.html (last visited Oct. 5, 2017).

[12] *See, e.g.*, Soma, *supra*, at *3–*4.

24. The unauthorized disclosure of a person's social security number can be particularly damaging since social security numbers cannot be easily replaced like a credit card or debit card. A person whose PII has been compromised cannot obtain a new social security number unless he or she can show that the number is being used fraudulently.

25. Even if a victim were to obtain a new social security number, that would not absolutely prevent against identity theft. Government agencies, private businesses, and credit reporting companies likely maintain a victim's records under the old number, so using a new social security number will not guarantee a fresh start. For some identity-theft and identity-fraud victims, a new number may create new problems. Because prior, positive credit information is not associated with the new social security number, it is more difficult to obtain credit due to the absence of a credit history. Indeed, the Social Security Administration warns that "a new number probably won't solve all [] problems . . ." and "won't guarantee [] a fresh start."[13]

26. A person whose PII has been compromised may experience identity theft and identity fraud for years because PII is a valuable commodity to identity thieves, and once that information has been compromised, these criminals often trade the information on the "cyber black-market" for years, and possibly indefinitely.

27. A "phishing" scheme is an attempt to acquire personal information, such as usernames, passwords, credit card details, and other sensitive information, by masquerading as a trustworthy entity or individual through an electronic communication, such as e-mail. A "whaling" scheme—otherwise known as "CEO fraud" or "fake president fraud"—is a

[13] *See Identity Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited October 10, 2017).

variation of a "phishing" scheme. A "whaling" scheme specifically targets or impersonates high-ranking members of a company, with the usual goal being to trick the contacted employee into sending sensitive or personal information via an unsecure channel, such as e-mail.

28. During tax season, cybercriminals often use phishing or whaling attacks to steal W-2 data, which, in turn, is used in connection with tax-refund fraud. Cybercriminals may also sell the information underground (i.e., on the dark web) or use it to stage further attacks.

29. The risk of theft by, or disclosure to, cyber criminals of sensitive data, including PII, stored electronically is well-documented and common knowledge. In the information age, such attacks are commonplace and thus companies are, and/or should be, aware that they must take precautions to prevent becoming unwitting accomplices to these schemes, especially in light of numerous recent, high-profile attacks.

30. Indeed, companies nationwide, including various retailers, banks, hospitals, and other high-profile businesses, have been hit by highly-publicized phishing and whaling schemes in recent times.

31. Since the beginning of 2016, the following companies have publicized similar data breaches in which their employees' W-2 information was compromised and disclosed as a result of similar phishing scams: A&A Ready Mixed Concrete, Academy of Art Institute, Acronis, Actifio Inc., Advance Auto Parts, Agenus, Alpha Payroll Services, American Type Culture Collection, AmeriPride Services Inc., Applied Systems Inc., ARC International, ARIAD Pharmaceuticals, Ash Brokerage Corp., Aspect Software, ASPIRAnet, Asure

Software, Astreya Partners, Inc., Avendra, LLC, Avention (now Dun & Bradstreet (D&B)), Avinger, Inc., AxoGen, Inc., BackOffice Associates, Behavioral Science Technology, Ben Bridge Jeweler, Inc., Billy Casper Golf, BloomReach, BrightView, Bristol Farms, Brunswick Corporation (Brunswick Boat Group, Boston Whaler, Cybex International, Leiserv Inc., and Sea Ray Boats, Inc.), Care.com (and its subsidiaries), CareCentrix, Central Concrete Supply Co. (Right Away Redy Mix and Rock Transport, Inc.), Century Fence, Champlain Oil, Client Network Services, ConvaTec Inc., Convey Health Solutions, Conway Group, Crane Co., Dare Enterprises (via Blue Belt Technologies), DataXu Inc., DealerSocket Inc., Dennis Group, Digilant, Dixie Group, Dynamic Aviation, eClinicalWorks, EMSI (Examination Management Services, Inc.), Endologix Inc., EPTAM Plastics, Equian, LLC, Evening Post Industries, Fast Company, Foss Manufacturing Company, Gamesa Wind US, General Communication, Inc. (GCI, Denali Media, UUI, and Unicom), Gryphon Technologies, Haeco Americas LLC, I.M. Systems Group, IASIS HEALTHCARE LLC, Information Innovators Inc., Information Resources Inc., InvenSense, InVentiv Health, Inc., ISCO Industries, J. Polep Distribution Services, Kantar Group, Krispy Kreme, Lamps Plus and Pacific Coast Lighting, Land Title Guarantee Company, Lanyon Solutions, LAZ Parking, Magnolia Health Corporation, Main Line Health, Management Health Systems d/b/a MedPro Healthcare Staffing, Mansueto Ventures (on behalf of Inc.), Maritz Holdings, Inc., Masy Bioservices, Matric NAC and Matrix Service Company, MCM Staffing, Medieval Times, Mercy Housing, Inc., Michels Corporation, Mitchell International Inc., Milwaukee Bucks, MNP Corporation (on behalf of its affiliate, General Fasteners Company), Monarch Beverage Company, Moneytree, Morongo Casino, Nation's

Lending Corporation, NetBrain Technologies, Inc., Netcracker Technology, New Leaders, NTT Data, O.C. Tanner, OpSec Security, PerkinElmer, Pharm-Olam International, Pivotal Software, Inc., Polycom, Primary Residential Mortgage, Inc. (PRMI), Proskauer Rose, Puppet, Inc., Pure Integration, LLC, QTI Group, RagingWire Data, Rightside, RugDoctor, Ryman Hospitality Properties (Grand Ole Opry, WSM-AM, and Wildhorse Saloon Nashville's General Jackson Showboat), SalientCRGT, Santa Rosa Consulting, Seagate Technology, SevOne, Silicon Laboratories, Single Digits, Snapchat, Spectrum, Inc., Sprouts, Tom McLeod Software Corps, Total Community Options Inc. d/b/a InnovAge, Turner Construction, VBrick Systems, Verity Health System, Veterans Management Services, Inc., Whiting-Turner Contracting Company, WorkCare, Wynden Stark, d/b/a GQR Global Markets/City Internships, York Hospital, and YourEncore.

32. In light of these well-documented data breaches, Lincare knew, or should have known, that it was susceptible to such an attack, and that it needed to implement and maintain adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect the sensitive and confidential information with which it was entrusted.

33. Additionally, the IRS and the FBI have published warnings over the last several years regarding the prevalence of malicious phishing e-mails being sent to individuals and companies to steal personal information.

34. On August 27, 2015, the FBI issued a public service announcement ("PSA") entitled "Business Email Compromise," therein detailing and warning of the extent of cyber-fraud incidents occurring to American businesses nationwide, as well as suggesting that

businesses take steps to protect themselves, such as by exercising more careful scrutiny over e-mail requests, and using multi-factor authentication, including telephone verification, to verify e-mail requests.[14]

35. On February 18, 2016, the IRS issued a public advisory warning after reporting an approximate 400 percent increase in phishing and other similar malicious incidents during the year's tax season. These phishing e-mails are designed to look like official communications from the IRS or others in the tax industry, such as tax software companies. The e-mails typically ask individuals to update important information by clicking on a web link. The link then takes the individual to a scam web-page designed to look like an official page from the IRS or some other tax-industry company or professional. Individuals who do not detect the fraudulent nature of the e-mail and the web link end up disclosing their personal information, such as their social security number, to an unauthorized third-party or parties, who then uses the information for a variety of illegal activities, such as filing false tax returns to fraudulently obtain tax refunds.

36. On March 1, 2016, the IRS issued a public-advisory warning to payroll and HR professionals specifically, alerting them to be aware of an emerging phishing e-mail scheme whereby a purported company executive requests employees' personal information. The IRS reported that the payroll and HR departments at several other companies had already received and responded to such e-mails and had disclosed their employees' W-2s, containing social security numbers and other PII, to cybercriminals posing as company executives. The

[14] *See Business Email Compromise*, Federal Bureau of Investigation, https://www.ic3.gov/media/2015/150827-1.aspx (last visited October 10, 2017).

IRS statement warned companies to check out e-mails that appear to come from company executives, and ask for personal information regarding company employees, to ensure that such requests for information are legitimate before responding. This variation of phishing is called a "spoofing" e-mail.

37. On April 4, 2016, the FBI's Phoenix, Arizona office published a news bulletin entitled "FBI Warns of Dramatic Increase in Business E-Mail Scams," wherein it highlighted the dramatic and ever-increasing extent of e-mail fraud schemes, and the substantial effects such schemes were having on businesses and victims in each state nationwide.[15] The FBI's bulletin noted the "great lengths" schemers go to in perpetrating their fraudulent schemes, highlighted the 270% increase in identified victims and exposed losses resulting from such schemes, and provided resources and tips for businesses to protect themselves, including exercising greater scrutiny of e-mail requests, making telephone calls to verify e-mail requests, and practicing multi-level authentication.

38. On June 14, 2016, the FBI issued another PSA entitled "Business E-Mail Compromise: The 3.1 Billion Dollar Scam."[16] This PSA noted that the Business E-mail Compromise ("BEC") scheme "continues to grow, evolve, and target businesses of all sizes," and critically identified a "new" BEC scenario presenting a distinct risk to businesses—Data Theft involving PII and W-2 information—which "first appeared just prior to the 2016 tax season." To that end, the FBI warned:

---

[15] *See* Jill McCabe, *FBI Warns of Dramatic Increase in Business E-Mail Scams*, FBI PHOENIX, https://www.fbi.gov/contact-us/field-offices/phoenix/news/press-releases/fbi-warns-of-dramatic-increase-in-business-e-mail-scams (last visited October 10, 2017).

[16] *See Business E-Mail Compromise: The 3.1 Billion Dollar Scam*, Federal Bureau of Investigation, https://www.ic3.gov/media/2016/160614.aspx (last visited October 10, 2017).

> Based on [Internet Crime Complaint Center] complaints and other complaint data, there are five main scenarios by which this scam is perpetrated. BEC victims recently reported a new scenario (Data Theft) involving the receipt of fraudulent e-mails requesting either all Wage or Tax Statement (W-2) forms or a company list of Personally Identifiable Information (PII).
>
> * * *
>
> **Scenario 5 (New): Data Theft**
>
> Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entity in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipient of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario, even if they were able to successfully identify and avoid the traditional BEC incident. The data theft scenario (Scenario 5) of the BEC first appeared just prior to the 2016 tax season.

Regarding "suggestions for protection and best practices," the FBI specifically recommended that businesses take the following steps to prevent falling victim to e-mail fraud schemes:

> Businesses with an increased awareness and understanding of the BEC scam are more likely to recognize when they have been targeted by BEC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.
>
> Businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting BEC attempts.
>
> Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request.
>
> The following is a compilation of self protection strategies provided in the BEC PSAs from 2015.
>
> - Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.

- Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and financial security procedures, including the implementation of a 2-step verification process. For example -
  - Out of Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this second-factor authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.
  - Digital Signatures: Both entities on each side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.
  - Delete Spam: Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
  - Forward vs. Reply: Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient's correct e-mail address is used.
  - Consider implementing Two Factor Authentication (TFA) for corporate e-mail accounts. TFA mitigates the threat of a subject gaining access to an employee's e-mail account through a compromised password by requiring two pieces of information to login: something you know (a password) and something you have (such as a dynamic PIN or code).

39. Finally, as indicated by another PSA published by the FBI on May 4, 2017, entitled "Business Email Compromise E-Mail Account Compromise The 5-Billion Dollar Scam," e-mail fraud schemes directed at businesses had increased by 61.3% since the time of

the FBI's last update 10 months earlier, on June 14, 2016, which timeframe included the Lincare Data Breach.[17]

40. Based upon these explicit warnings by the IRS and FBI alone—particularly in combination with the numerous, similar data-breaches nationwide in recent months, and Lincare's recent HIPAA violation involving failure to safeguard records containing patients' personal-health information—Lincare was placed on notice that it needed to implement and maintain adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect the sensitive and confidential information with which it was entrusted.

B. Background on Lincare

41. Incorporated in 1990, Lincare is one of the nation's largest providers of oxygen, respiratory, and other chronic-therapy services to patients in the home. Its customers typically suffer from chronic, obstructive pulmonary disease, such as emphysema, chronic bronchitis, or asthma, and require supplemental oxygen, respiratory, and other chronic-therapy services in order to alleviate the symptoms and discomfort of respiratory dysfunction. Lincare serves hundreds of thousands of customers in 48 U.S. states and Canada through its over 14,000 employees operating in over 1,000 locations.

42. Lincare, as an employer, required Plaintiffs and the Class Members to surrender to it their social security numbers and other PII. Indeed, Lincare collects and stores its employees' PII, including full names, addresses, social security numbers, wages, and

[17] *See* Business E-Mail Compromise E-Mail Account Compromise The 5 Billion Dollar Scam, Federal Bureau of Investigation, https://www.ic3.gov/media/2017/170504.aspx (last visited October 10, 2017).

withheld taxes, which are included on IRS Form W-2s, for distribution to employees and tax authorities, and was entrusted with properly holding, safeguarding, and protecting such information against harm, including improper disclosure and misuse.

43. Lincare also required Plaintiffs and the Class Members to surrender to it the social security numbers and other PII of other individuals, such as their families, dependents, and/or designated beneficiaries of employment-related benefits through Lincare. Such information was provided, *inter alia*, as information concerning beneficiaries for retirement plans, health insurance coverage, or other insurance plans.

44. Accordingly, and because employees and former employees (as well as their families, dependents, and/or designated beneficiaries) were foreseeable and probable victims of any inadequate security practices and had no ability to protect their PII that was in Lincare's possession, Lincare owed a duty of care to ensure that such PII was not disseminated, accessed, or used for improper purposes, and further owed fiduciary and contractual duties to ensure the same. Lincare's duties included, *inter alia*, establishing, maintaining, and ensuring adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect PII from wrongful disclosure, as well as training employees with access to PII as to the same. Lincare knew that by collecting and storing its employees' sensitive and confidential PII, it undertook such responsibilities.

45. Lincare itself is no stranger to breaches of confidential and sensitive personal data that it has been entrusted to safeguard and protect. Because Lincare is a healthcare company that collects patient-identifiable health information, it is subject to HIPAA and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which

require Lincare to comply with standards for the use and disclosure of health information internally within Lincare, as well as with third-parties. Nevertheless, as recently as January 13, 2016, the United States Department of Health and Human Services, Office for Civil Rights, determined that Lincare violated HIPAA, and imposed a $239,800 civil fine, for Lincare's failure to implement policies and procedures to safeguard records containing its patients' protected health information.

46. Based upon this breach of HIPAA, Lincare was placed on specific notice that it needed to implement and maintain a more adequate and reasonable data security processes, controls, policies, procedures, and protocols to safeguard and protect the sensitive and confidential information with which it was entrusted.

47. At all times relevant to this Complaint, Lincare should have been, and was, actually advised by skilled lawyers, employees, and other professionals who were, or should have been knowledgeable, about protection and storage of PII.

C. The Lincare Data Breach

48. On February 3, 2017, an employee working in Lincare's HR department received an e-mail from a criminal purporting to be a Lincare executive-level employee. In this e-mail, the purported executive requested that the HR employee send him or her the W-2 information of Lincare employees. The Lincare HR employee, rather than confirming or authenticating the validity of the request, compiled the requested information and complied with the request by e-mailing the name, address, social security number, earnings information, and more, of current and former Lincare employees to the purported Lincare

executive, thus, initiating the Data Breach. Lincare did not have the most basic security protocols or checks in place to prevent the Data Breach from occurring.

49. Thereafter, sometime between February 3, 2017 and February 10, 2017, Lincare discovered that the e-mail from the purported Lincare executive was actually a whaling scheme, and that the HR employee had improperly disclosed the unencrypted PII of current and former Lincare employees to an unauthorized third-party or parties. As a result, Lincare released and disclosed Plaintiffs' and the Class Members' PII, including their names, addresses, social security numbers, earnings information, and more, to an unauthorized third-party or parties and, potentially, the public.

50. Despite the IRS' and FBI's explicit warnings, the numerous, similar data breaches nationwide in prior months, and Lincare's recent HIPAA issue involving failure to safeguard records containing patients' personal health information, Lincare did not encrypt or password-protect any of the Plaintiffs' PII that it wrongfully disclosed.

51. Sometime between February 3, 2017 and February 10, 2017, Lincare became aware of the Data Breach disclosing its employees' PII and W-2 information.

52. About a week later, on or about February 10, 2017, Lincare notified current and former employees about the Data Breach via e-mail. This e-mail, and corresponding attachment, stated, *inter alia*, that Lincare had disclosed the PII of current and former employees—including names, addresses, social security numbers, earnings information, and other general, related information—to a criminal when fulfilling a request for W-2 information from said criminal pretending to be one of Lincare's executive-level employees.

53. The February 10, 2017 email and attachment stated that Lincare would be offering a complimentary two-year membership for InfoArmor identity protection services. As discussed below, this measure did little to protect the PII that had already been disclosed to third-parties.

54. The February 10, 2017 email and attachment also claimed that Lincare had re-trained and re-educated its HR and Payroll staff, including the HR employee involved in the information release, on the importance of remaining vigilant about these types of criminal attacks.

55. The February 10, 2017 e-mail notification and attachment were signed by Juan de la Cruz Beltran, Lincare's Head of Human Resources.

56. Approximately a month later, Lincare sent, by mail, a Frequently Asked Questions ("FAQ") document, dated March 13, 2017. This letter did not provide a fuller account of the incident (as the February 10, 2017 e-mail notification claimed it would), and did not confirm the degree to which Lincare's current and former employees had been affected.

57. Finally, on or about April 21, 2017, Plaintiffs received another letter from Lincare, by mail, which warned that current and/or former employees affected by the Data Breach had already had their PII used by a third-party or parties as part of a fraudulent scheme to obtain federal student loans through the Department of Education's Free Application for Federal Student Aid.

58. Plaintiffs have received no further documentation or communication from Lincare since the April 21, 2017 letter.

59. Lincare claims to have offered current and former employees two years of credit monitoring and insurance through InfoArmor, but this minor half-measure did not safeguard and protect the already-released PII. Credit monitoring and insurance cannot prevent identity theft or fraud, even for a two-year period. Credit monitoring only informs a consumer of instances of fraudulent opening of new accounts, and identity theft insurance reimburses losses after they have occurred. Neither prevent identity theft or fraud by: (i) detecting sales of W-2 tax information on the black market before the information is used to commit identity theft or identity fraud; (ii) monitoring public records, loan data, or criminal records; (iii) flagging existing accounts for fraud in order to prevent identity thieves' use of compromised W-2 tax information before an unauthorized transaction can be completed; or (iv) freezing credit, which prevents identity thieves' ability to open new accounts with compromised W-2 tax information.

60. Websites ranking companies that provide identity-protection services have noted that while many of such companies do offer services to prevent identity theft and fraud, InfoArmor's services (ranked just 33rd overall by one rankings website) use only one-bureau (TransUnion) credit monitoring, while many other services offer all three credit bureaus, and moreover, offer just one credit report annually.[18]

61. The e-mail notification and letters Lincare sent to Plaintiffs on February 10, 2017, March 13, 2017, and April 21, 2017, respectively, squarely placed the burden on Plaintiffs and the Class Members, rather than Lincare, to protect themselves and mitigate the damages flowing from the Data Breach, such as spending time and money reviewing their

[18] *See InfoArmor Review*, Identity Theft Protection Bureau, http://www.itpbureau.com /reviews/infoarmor/ (last visited Oct. 6, 2017).

account statements and monitoring their credit reports, as well as resolving fraudulent uses of their PII, such as fraudulent tax return filings, loan and credit applications, bank fraud, and other forms of identity theft. Unfortunately, many of Lincare's mitigation directives require Plaintiffs and the Class Members to incur additional out-of-pocket expenses and spend hours of their personal time on such actions. For example, as a general rule in Florida, the fee to place (and remove) a "security freeze" on one's credit report is approximately $10 each time it is placed with each of the three credit reporting agencies (Experian, Equifax, and Transunion). Monitoring one's credit reports, an option explicitly encouraged by Lincare's email and letters, would cause a Data Breach victim to incur an expense to see his or her credit reports beyond the one, free annual report to which they are entitled. Lincare has not offered to pay for the cost of these protections, despite the fact other companies similarly affected by data breaches have offered to reimburse such costs.

62. Further, the PII "protection" offered by Lincare is woefully inadequate because the free credit monitoring and identity-theft insurance lasts for only two years. As advised by the FTC and data theft experts, a person impacted by a data breach should continue to take proactive steps well after two years have passed to protect against identity theft and related fraud because cybercriminals are aware that two years is a common duration for credit monitoring following a data breach, and therefore may wait until that period of credit monitoring has elapsed before using the stolen PII for fraudulent means or sale on the black market.

63. Lincare's response to the Data Breach is also inadequate because it places the burden on Plaintiffs and the Class Members to monitor, protect against, and resolve issues

stemming from the Data Breach, especially following the two-year period of protection offered through InfoArmor. Additionally, while Plaintiffs and the Class Members were automatically enrolled by Lincare in certain protection services through InfoArmor, Lincare sent instructions to those affected, recommending that they affirmatively enroll in an extended-coverage plan through InfoArmor to receive numerous other critical aspects of protection, including receipt of monthly credit scores, annual credit reports, financial monitoring, compromised credential protection, wallet protection, social monitoring, password protection, solicitation reduction, digital exposure reports, and other additional resources. This clear attempt by Lincare to mitigate the costs associated with the Data Breach is likewise inadequate because it again pushes the burden from Lincare, whose actions (or rather inaction) caused the Data Breach to occur, onto the backs of its current and former employees to protect their own PII.

64. Additionally, after Plaintiffs and the Class Members sign up for the credit-monitoring program and provide the three credit bureaus with their contact information, the credit bureaus will most certainly solicit them with advertising to purchase other products and services Lincare decided not to provide, or a continuation of the short program that Lincare did offer. These advertisements will serve to further exploit Plaintiffs and the Class Members.

65. Lincare had duties—including, without limitation, those arising from its position as an employer and a fiduciary, as well as those arising from its employment agreements with Plaintiffs and the Class Members—to guard and protect the private, highly sensitive, confidential PII of Plaintiffs and the Class Members.

66. Indeed, Lincare provided employment handbooks to its employees, which state, in pertinent part, as follows:

> **CONFIDENTIALITY**
>
> ***Information revealed and services performed during the course of employment at Lincare shall be kept confidential and remain confidential.*** Under no circumstances may any Lincare employee use information that he learned in the course of his employment with Lincare for personal gain, personal use or personal business. ***Disclosing confidential information to persons not entitled to such information and/or assisting others in gaining unauthorized access to Lincare records or information are clear violations of this Policy.*** The communication of false or malicious information about Lincare, its customers or its employees is also a violation of this Policy.

Accordingly, Lincare created an expectation of privacy for its employees' confidential information, but failed to follow through with its duty to safeguard and protect the same.

67. Even in the face of this provision (the "Confidentiality Provision"), the IRS' and FBI's explicit warnings regarding these types of phishing schemes, the numerous, similar data breaches that had recently occurred nationwide, and Lincare's recent HIPAA issue involving failure to safeguard records containing patients' personal health information, Lincare did not implement adequate and reasonable security measures to safeguard and protect against a breach and/or disclosure of its current and former employees' PII.

68. Lincare knew, or should have known, that its data security processes, controls, policies, procedures, and protocols were insufficient, inadequate, and did nothing to safeguard and protect its current and former employees' PII, yet Lincare did nothing to expand, improve, update, or ensure them.

69. Indeed, the Data Breach could have been prevented, or greatly minimized, had Lincare utilized the proper data security measures, processes, controls, policies, procedures,

and protocols. Lincare recognized as much, as it asserted in its February 10, 2017 e-mail notification that it was working to enhance its controls by re-educating and re-training its HR and Payroll staff, including the involved HR employee.

70. The Data Breach could have been prevented had Lincare implemented securely-configured mail services with advanced spam filters so that the phishing e-mail never reached the HR employee's inbox in the first place.

71. The Data Breach could have been prevented had Lincare conducted sufficient information-security training throughout Lincare. Lincare should have provided adequate and reasonable education and training to its HR employees, as well as any other employees with access to employees' PII, as follows: (i) to be aware of the signs of fraudulent e-mail scams; (ii) to verify the sources of e-mail messages that are sent to them and that ask for sensitive company or personal information; (iii) to question requests for PII and other sensitive information that are made through informal or non-routine channels; (iv) to alert key members of the company if a request for information seems suspicious; and (v) to ask questions before responding when presented with what appears to be a request from a company executive for employee PII, such as contacting the company executive via telephone to ensure the request is legitimate, or inquiring as to why non-finance personnel "need to know" the data requested.

72. The Data Breach also could have been prevented had Lincare implemented data-security controls, policies, and procedures regarding HR employees' access to employee PII. Lincare should have had policies in place that prohibited HR employees from having on-demand access to all of its employees' PII, or at least required HR employees to go

through multiple layers of computer-system security, scrutiny, and/or authentication, such as requiring express approval from a superior, or involving the information technology or security team before being provided access to so much sensitive information at one time.

73. The Data Breach could have been prevented had Lincare implemented data-security measures to ensure that employee PII was never sent in an unencrypted form. Lincare should have used proper controls for data access and encrypted employee information that was sent via e-mail, so that it could maintain control of the data, even after it was sent. In addition, Lincare should have implemented a data-security measure that provided it with the capability to remotely delete a file that was mistakenly sent.

74. But Lincare violated basic guidelines to encrypt or password-protect sensitive information of its employees, and in so doing, failed to meet the most basic standards of data security and reasonable business practices, and thereby failed to ensure adequate security of Plaintiffs' and the Class Members' PII, and failed to retain this PII in a secure and safe manner.

75. Had Lincare taken even these most fundamental data-security measures, the Data Breach never would have happened.

76. Lincare failed to take reasonable precautions to protect the PII of Plaintiffs and the Class Members, and otherwise failed to act reasonably in fulfillment of their duties not to disclose the PII of Plaintiffs and the Class Members, and to affirmatively safeguard and protect that PII.

77. Lincare not only failed to safeguard and protect Plaintiffs' and the Class Members' PII, but voluntarily handed it over to a third-party or parties upon their mere e-mail request.

78. Lincare recklessly, negligently, and carelessly maintained its current and former employees' PII.

D. The Harm Suffered by Plaintiffs

79. As a result of the Data Breach, an unknown third-party or parties now possess the PII of Lincare's current and former employees, all of whom are the Plaintiffs and Class Members in this case.

80. Within just weeks of the Data Breach, certain Plaintiffs' PII was used to steal their federal tax returns, to wreak havoc on their tax filings, and to cause unmeasured damage to their identities, which damage is ongoing.

81. On or about March 16, 2017, Plaintiff Giancola, a former Lincare employee, received a letter from the IRS notifying him that a federal tax return had been filed using his name and social security number. In response, Giancola contacted the IRS and informed it that he had not filed that tax return, and accordingly, that the return had been fraudulently filed by an imposter.

82. As a result of this tax fraud, Giancola hired an accountant from Fredrick James Tax & Accounting to file a proper tax return on his behalf, which the accountant filed in or about April 2017. After filing the proper tax return, Giancola received a notice from the IRS indicating that his proper tax return could not be processed because the false tax return had been filed using his name and social security number.

83. Shortly thereafter, Giancola received another communication from the IRS informing him that yet another tax return had been filed using his name and social security number (i.e., by another imposter). Giancola again responded to the IRS and informed it that he had not filed this tax return either, and that it was, in fact, a second fraudulent filing.

84. Giancola and his accountant proceeded to work with the IRS for several hours over the course of the next few months, requiring Giancola to prove his identity and that the two other tax returns filed using his name and social security number were, in fact, fraudulent.

85. Finally, in or about August 2017, Giancola successfully proved his identity and that the two tax returns filed by the imposters were fraudulent, and received his federal tax refund.

86. Giancola had never before hired an accountant to review or file his federal taxes, and only hired the accountant as a result of the tax fraud caused by the Data Breach. Giancola has spent approximately $598 on the accountant's services, and has spent numerous hours working with the accountant and the IRS to properly file his taxes, rectify the tax fraud, and receive his tax refund.

87. The credit-monitoring service provided by Lincare through InfoArmor has not alerted Giancola at any time that the fraudulent tax returns were filed using his name and social security number.

88. As a result of the Data Breach, Giancola's social security number and other PII has been compromised, and it will require additional time, money, and effort to monitor his credit reports and bank accounts, and repair the damage already done, and that likely will

be done, every year for the rest of his life to ensure that his social security number is not used again, and to do, or undo, whatever is necessary to rectify the damage caused by the Data Breach. Giancola, like all Plaintiffs and Class Members, suffers from a distinctly-increased risk of future identity theft as a result of Lincare's actions and/or inactions. Giancola has already expended several hours attempting to safeguard himself from identity theft and other harms caused by the release of his PII, including his social security number and W-2 tax information, and he continues to do so every month, and will have to continue doing so for the foreseeable future. Going forward, Giancola anticipates spending considerable time and money in an effort to contain the impact of Lincare's Data Breach on himself.

89. Likewise, Plaintiff Smith has already had her identity stolen. Smith filed her federal tax return with the IRS in or about April 2016. The very next day, Smith was informed that the IRS would not accept her federal tax return because a federal tax return had already been filed using her name and social security number.

90. As a result of, and in response to, this tax fraud, Smith contacted the IRS and informed it that she had not filed that tax return, and accordingly, that the return had been fraudulently filed by an imposter.

91. Smith also reported the tax fraud to the Sheriff's Department of Pinellas County, Florida, which opened a case and investigation into the tax fraud. At the recommendation of the Pinellas County Sheriff's Department, Smith placed a freeze on her credit reports with each of the three credit bureaus (Experian, Transunion, and Equifax).

92. Smith proceeded to work with the IRS and Sheriff's Department, as well as the FTC, for several hours over the course of the next several months, requiring Smith to

prove her identity and that the tax returns filed using her name and social security number were, in fact, fraudulent.

93. Finally, in or about August 2017, Smith successfully proved her identity and that the tax return filed by the imposter was fraudulent, and received her federal tax refund.

94. Smith has spent numerous hours working with the IRS and the Pinellas County Sheriff's Department to properly file her taxes, rectify the tax fraud, and receive her tax refund.

95. The credit monitoring service provided by Lincare through InfoArmor has not alerted Smith at any time that the fraudulent tax return was filed using her name and social security number.

96. As a result of the Data Breach, Smith's social security number and other PII has been compromised, and will require additional time, money, and effort to monitor her credit reports and bank accounts, and repair the damage already done, and that likely will be done, every year for the rest of her life to ensure that her social security number is not used again, and to do, or undo, whatever is necessary to rectify the damage caused by the Data Breach. Smith, like all Plaintiffs and Class Members, suffers from a distinctly-increased risk of future identity theft as a result of Lincare's actions and/or inactions. Smith has already expended several hours attempting to safeguard herself from identity theft and other harms caused by the release of her PII, including her social security number and W-2 tax information, and she continues to do so every month, and will have to continue doing so for the foreseeable future. Going forward, Smith anticipates spending considerable time and money in an effort to contain the impact of Lincare's Data Breach on herself.

97. Plaintiff Scott has also suffered adverse impacts as a result of the Data Breach. Scott was forced to contact, and spend significant time working with, the IRS to file a Form 14039 (Identity Theft Affidavit) to place an alert on his tax return, so that others could not file another tax return in 2016 using his name and social security number. As a result, Scott's 2016 federal tax refund, which he filed jointly with his wife (as he does every year) was delayed.

98. As a result of the Data Breach, Scott's social security number and other PII has been compromised, and will require additional time, money, and effort to monitor his credit reports and bank accounts, and repair the damage already done, and that likely will be done, every year for the rest of his life to ensure that his social security number is not used improperly, and to do, or undo, whatever is necessary to rectify the damage caused by the Data Breach. Scott, like all Plaintiffs and Class Members, suffers from a distinctly-increased risk of future identity theft as a result of Lincare's actions and/or inactions. Scott has already expended several hours attempting to safeguard himself from identity theft and other harms caused by the release of his PII, including his social security number and W-2 tax information, and he continues to do so every month, and will have to continue doing so for the foreseeable future. Going forward, Scott anticipates spending considerable time and money in an effort to contain the impact of Lincare's Data Breach on himself.

99. Due to Lincare's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Plaintiffs and the Class Members have been, and will continue to be, required to take affirmative and/or corrective steps to recover their peace of mind and personal security, for which there is a substantial financial and temporal cost.

Plaintiffs and the Class Members will spend significant time and expense engaging in such actions, including, without limitation: (i) identifying and dealing with fraudulent charges and accounts, including tax refund fraud, fraudulent credit applications, and fraudulent student loan applications; (ii) frequently purchasing credit reports from multiple credit-reporting agencies; (iii) placing and removing fraud alerts and security freezes on credit reports; (iv) purchasing credit monitoring and internet monitoring services; (v) purchasing identity-theft insurance; (vi) spending time on the telephone, internet, and in-person attempts to sort out issues related to the Data Breach; and (vii) even obtaining new social security numbers.

100. As a direct and proximate result of Lincare's disclosure of its employees' PII, including their social security numbers and W-2 information, the Plaintiffs' and Class Members' PII was stolen and used to claim Giancola's and Smith's tax refunds, delay Scott's tax refund, and as yet, impact an unknown number of Class Members' tax refunds, as well as to submit fraudulent student loan applications and/or credit applications using the PII of the Class Members.

101. Lincare grossly and flagrantly disregarded and violated Plaintiffs' and the Class Members' rights, and harmed them in the process, by failing to safeguard and protect and, in fact, wrongfully releasing and disclosing, their PII to an unauthorized third-party or parties, and potentially the public, without their authorization.

102. Lincare grossly and flagrantly disregarded and violated Plaintiffs' and the Class Members' rights, and harmed them in the process, by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit the appropriate data-security processes, controls, policies, procedures, and protocols to safeguard and protect Plaintiffs'

and the Class Members' PII. Lincare's failure to do so—even in the face of the numerous, similar data breaches nationwide in recent months, the IRS' and FBI's warnings to beware of, and protect against, such breaches, and Lincare's recent HIPAA violation involving failure to safeguard and protect patients' personal health information—is an abuse of discretion, and confirms its intentional and/or grossly negligent failure to observe procedures required by law and industry standards and recommendations.

103. Lincare grossly and flagrantly disregarded and violated Plaintiffs' and the Class Members' rights, and harmed them in the process, by depriving them of the value of their PII, for which there is a national and international market in which cybercriminals sell and trade the stolen PII.

104. As a direct and proximate result of Lincare's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Plaintiffs and the Class Members have incurred, and will continue to incur, economic damages, other injury, and actual harm, including but not limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII, entrusted to Lincare for the purpose of deriving employment from Lincare and with the understanding that Lincare would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts; (5) lost opportunity costs associated with effort expended, and the loss of

productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity-data misuse; (6) costs associated with the ability to use credit, and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised PII to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts, and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, which remains in Lincare's possession and is subject to further breaches so long as Lincare fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members, and potentially, their families, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, all of which have an ascertainable monetary value to be proven at trial.

105. The Data Breach is a substantial cause of the identity theft and tax fraud already suffered by Plaintiffs Giancola and Smith.

CLASS ACTION ALLEGATIONS

106. Plaintiffs bring claims pursuant to Fed. R. Civ. P. 23 on behalf of a class of similarly situated persons, which they initially propose be defined as follows:

> **All current and former employees of Lincare who, during the period beginning on or about February 10, 2017 and continuing through the present, had their PII, including names, addresses, social security numbers, and/or W-2 information, wrongfully and voluntarily disseminated by Lincare to a third party or parties.**

107. **Numerosity**. The exact number of Class Members is unknown to Plaintiffs at this time, but upon information and belief, there are likely hundreds, if not thousands, of Class Members dispersed throughout the country. Indeed, as of September 2017, Lincare had approximately 14,000 active employees. Accordingly, the proposed Class is sufficiently numerous, and joinder of all Class Members is impracticable. The Class Members can be readily identified through records maintained by Lincare.

108. **Commonality**. Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class Members, including the following issues:

a. whether Lincare received and stored the PII of Plaintiffs and the Class Members;

b. whether Lincare had a duty to use reasonable security measures to protect the Plaintiffs' and Class Members' PII;

c. the standard to which Lincare is to be held with respect to its possession and/or dissemination of the PII of Plaintiffs and the Class Members;

d. whether Lincare adequately designed, adopted, implemented, controlled, directed, oversaw, managed, monitored, and audited the appropriate data-security processes, controls, policies, procedures, and protocols to safeguard

and protect the PII of Plaintiffs and the Class Members that was disclosed without authorization in the Data Breach;

e. whether Lincare failed to act reasonably in protecting the PII of Plaintiffs and the Class Members in its care, custody, and control;

f. whether the actions, and/or failures to act, of Lincare caused the PII of Plaintiffs and the Class Members to be disseminated, accessed, and/or stolen without authorization;

g. whether Lincare was negligent;

h. whether Lincare's conduct with respect to the Data Breach was unfair and/or deceptive, in violation of the laws of Florida, including FDUTPA, Fla. Stat. § 501.201, *et seq.*;

i. whether Lincare breached its agreements, express and/or implied, with Plaintiffs and the Class Members;

j. whether Lincare violated a duty of good faith and fair dealing in its agreements with Plaintiffs and the Class Members;

k. whether Lincare owed a fiduciary duty to Plaintiffs and the Class Members as their employer;

l. whether Lincare breached a fiduciary duty it owed to Plaintiffs and the Class Members;

m. whether Plaintiffs and the Class Members are at an increased risk of identity theft as a result of Lincare's breaches and failure to protect the PII of Plaintiffs and the Class Members;

n. whether Plaintiffs and the Class Members suffered injury, and/or will likely suffer injury, including ascertainable losses, as a result of Lincare's actions, inaction, omission, and want of ordinary care;

o. whether Plaintiffs and the Class Members are entitled to damages, and, if so, the nature of such damages;

p. whether Plaintiffs and the Class Members are entitled to recover attorneys' fees and expenses, and/or costs of litigation;

q. whether Lincare's actions constitute intentional misconduct and/or were grossly negligent; and

r. whether Plaintiffs and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

109. **Typicality**. Plaintiffs' claims are typical of the claims of the Members of the proposed Class because, among other things, Plaintiffs and the Class Members sustained similar injuries as a result of Lincare's uniform wrongful conduct—to wit, Lincare's failure to adequately safeguard and protect, and Lincare's unlawful disclosure of, the PII of Plaintiffs and the Class Members—which injuries were directly and proximately caused by Lincare's acts and omissions.

110. **Adequacy**. Plaintiffs will fairly and adequately protect the interests of the proposed Class. Their interests do not conflict with the Class Members' interests, and they have retained counsel experienced in complex class action litigation to prosecute this case on behalf of the Class.

111. **Superiority (pursuant to Fed. R. Civ. P. 23(b)(3))**. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class Members, and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing Lincare's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

112. **Fed. R. Civ. P. 23(b)(2)**. Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Defendant has acted on grounds generally applicable to the entire Class with respect to the matters complained of herein, thereby making appropriate the relief sought herein with respect to Class Members as a whole.

CAUSES OF ACTION

COUNT I
Negligence

113. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

114. Plaintiffs and the Class Members are, or were, employed by Lincare and were issued W-2s from Lincare, or for whom Lincare had W-2 data. As a condition of their employment, Plaintiffs and the Class Members were obligated to provide Lincare with

certain PII, including their names, addresses, and social security numbers, among other information.

115. Plaintiffs and the Class Members entrusted Lincare with their PII with the understanding that Lincare would safeguard and protect their information, and that Lincare was in a position to safeguard and protect against the harm suffered by Plaintiffs and the Class Members as a result of the Data Breach.

116. Defendant owed a duty of care to Plaintiffs and the Class Members to ensure that their PII was not disseminated, accessed, or used for improper purposes. This duty included, *inter alia*, establishing, maintaining, and testing data-security processes, controls, policies, procedures, and protocols to safeguard and protect the PII from wrongful disclosure, and training employees who had access to the PII as to the same. Lincare knew that by collecting and storing its employees' sensitive, personal and financial information, it undertook such a responsibility.

117. Lincare owed such a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate security practices. Plaintiffs and the Class Members had no ability to protect their data that was in Lincare's possession.

118. Lincare knew, or should have known, that it had inadequately safeguarded its employees' private tax information and social security numbers, and yet Lincare failed to take reasonable precautions to safeguard current and former employees' private tax information and social security numbers.

119. Lincare's own conduct also created a foreseeable risk of harm to Plaintiffs and the Class Members. Lincare's misconduct included, but was not limited to, its failure to take

the steps and opportunities to prevent and stop the wrongful disclosure of Plaintiffs' and the Class Members' PII, as set forth herein. Lincare's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the private tax information and social security numbers of Plaintiffs and the Class Members.

120. Defendant breached their duty of care to Plaintiffs and the Class Members to ensure that their PII was not disseminated or used for improper purposes by failing to adequately and reasonably safeguard and protect the PII, by voluntarily disseminating the PII, and by allowing the PII to be accessed, in unencrypted format, by a third-party or parties.

121. As a direct and proximate result of Lincare's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Plaintiffs and the Class Members have incurred, and will continue to incur, economic damages, other injury, and actual harm, including but not limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII, entrusted to Lincare for the purpose of deriving employment from Lincare and with the understanding that Lincare would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts; (5) lost opportunity costs associated with effort expended, and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect,

contest, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised PII to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, which remains in Lincare's possession and is subject to further breaches so long as Lincare fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members, and potentially, their families, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, all of which have an ascertainable monetary value to be proven at trial.

122. But for Lincare's failure to implement and maintain adequate security measures to protect their employees' PII and allowing unauthorized access to their employees' PII, the PII of Plaintiffs and the Class Members would not have been injured, and Plaintiffs and the Class Members would not be at a heightened risk of identity theft in the future. Lincare's negligence was a substantial factor in causing harm to Plaintiffs and the Class Members.

123. Lincare admitted that PII of Plaintiffs and the Class Members was wrongfully disclosed as a result of the Data Breach.

124. In addition, Lincare's current and former employees provided Lincare with PII of other individuals, such as their families, dependents, and/or designated beneficiaries of employment-related benefits through Lincare. Such information was provided, *inter alia*, as information concerning beneficiaries for retirement plans, health insurance coverage, or other insurance plans, and was likely compromised as part of the Data Breach.

125. Plaintiffs and the Class Members are entitled to monetary damages for all damages caused by Lincare's negligence. Plaintiffs also seek reasonable attorneys' fees and costs under the applicable law, including Fed. R. Civ. P. 23(h) and Fla. Stat. § 501.2105.

COUNT II
Breach of Fiduciary Duty

126. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

127. Lincare was a fiduciary, as an employer, and thus was required to act primarily for the benefit of its employees—to wit, Plaintiffs and the Class Members—in matters connected with their employment.

128. Plaintiffs and the Class Members were in a fiduciary relationship by way of the duty Lincare had in relation to the employment of Plaintiffs and the Class Members, and Lincare's duty to act for, or to give advice for, the benefit of Plaintiffs and the Class Members upon matters within the scope of their relationship, specifically, to keep income records, and report those records in a form W-2 to the IRS as the employer.

129. Lincare breached its duty of care to Plaintiffs and the Class Members to ensure that their PII and W-2s were not used for improper purposes by failing to provide adequate protections to the information, and by allowing the information to be accessed, in unencrypted format, by a third-party or parties to whom Lincare voluntarily disseminated such information.

130. As a direct and proximate result of Lincare's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Plaintiffs and the Class Members have incurred, and will continue to incur, economic damages and other injury and actual harm, including but not limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII, entrusted to Lincare for the purpose of deriving employment from Lincare and with the understanding that Lincare would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial accounts; (5) lost opportunity costs associated with effort expended, and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets; (7) unauthorized use of

compromised PII to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, which remains in Lincare's possession and is subject to further breaches so long as Lincare fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members, and potentially, their families, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, all of which have an ascertainable monetary value to be proven at trial.

COUNT III
Breach of Implied Contract

131. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

132. Lincare offered employment to Plaintiffs and the Class Members in exchange for compensation and other employment benefits. To receive compensation and other employment benefits, Lincare required Plaintiffs and the Class Members to provide their PII, including names, addresses, social security numbers, and other personal information.

133. Lincare had an implied duty of good faith to ensure that the PII of Plaintiffs and the Class Members in its possession was only used to provide the agreed-upon compensation and other employment benefits from Lincare.

134. Lincare was, therefore, required to reasonably safeguard and protect the PII of Plaintiffs and the Class Members from unauthorized uses.

135. Plaintiffs and the Class Members accepted Lincare's employment offer and fully performed their obligations under the implied contract with Lincare by providing their PII to Lincare, among other obligations.

136. Plaintiffs and the Class Members would not have provided and entrusted their PII to Lincare in the absence of their implied contracts with Lincare, and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from Lincare.

137. Lincare breached the implied contracts with Plaintiffs and the Class Members by failing to reasonably safeguard and protect the PII of Plaintiffs and the Class Members.

138. As a direct and proximate result of Lincare's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Plaintiffs and the Class Members have incurred, and will continue to incur, economic damages, other injury, and actual harm, including, but not limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII, entrusted to Lincare for the purpose of deriving employment from Lincare and with the understanding that Lincare would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial

accounts; (5) lost opportunity costs associated with effort expended, and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity-data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised PII to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and potentially, the PII of their family members, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, which remains in Lincare's possession and is subject to further breaches so long as Lincare fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class Members, and potentially, their families, dependents, and/or designated beneficiaries of employment-related benefits through Lincare, all of which have an ascertainable monetary value to be proven at trial.

COUNT IV
Violation of the Florida Deceptive and Unfair Trade Practices Act,
Fla. Stat. § 501.201, *et seq.*

139. Plaintiffs incorporate by reference and reallege each and every allegation contained above, as though fully set forth herein.

140. FDUTPA, Fla. Stat. § 501.201, *et seq.*, is expressly intended to protect "consumers" like Plaintiffs and the Class Members from deceptive, unfair, and unconscionable acts or practices in the conduct of trade or commerce.

141. Plaintiffs and the Class Members have a vested interest in the privacy, security, and integrity of their PII; therefore, this interest is a "thing of value" as contemplated by FDUTPA.

142. Defendant is a "person" within the meaning of FDUTPA and, at all pertinent times, was subject to the requirements and proscriptions of FDUTPA with respect to all of its business and trade practices described herein.

143. Plaintiffs and the Class Members are "consumers" "likely to be damaged" by Defendant's ongoing deceptive trade practices.

144. Defendant's unlawful conduct, as described in this Complaint, was directed and emanated from Defendant's headquarters to the detriment of Plaintiffs and the Class Members in Florida and throughout the United States.

145. Consumers, like Plaintiffs and the Class Members, entrusted Lincare with their PII as part of their employment agreements. Lincare accepted the trust reposed in it by its employees and implicitly agreed to keep this information safe. Lincare engaged in unfair and deceptive trade practices by representing to consumers like Plaintiffs and the Class Members that their PII would not be used without permission and, further, would be maintained in a manner consistent with current acceptable information security standards and practices. Lincare additionally engaged in unfair and deceptive trade practices when it

voluntarily transmitted its employees' PII to an unauthorized third-party or parties without first obtaining their consent.

146. Defendant violated FDUTPA by failing to properly implement adequate, commercially-reasonable security measures to safeguard and protect the sensitive PII of consumers—to wit, Plaintiffs and the Class Members—also in contravention of Florida's Information Privacy Act, Fla. Stat. § 501.171, which requires covered entities—i.e., companies, such as Lincare, which acquire, maintain, store, or use personal information, including individuals' names in combination with their social security numbers—to take reasonable measures to protect and secure data in electronic form containing personal information.

147. Plaintiffs and the Class Members have suffered ascertainable losses, as a direct result of Defendant's employment, of unconscionable acts or practices, and unfair or deceptive acts or practices.

148. Under FDUTPA, Plaintiffs and the Class Members are entitled to preliminary and permanent injunctive relief without proof of monetary damage, loss of profits, or intent to deceive. Plaintiffs and the Class Members seek equitable relief and to enjoin Defendant on terms that the Court considers appropriate.

149. Defendant's conduct has caused, and continues to cause, substantial injury to Plaintiffs and the Class Members. Unless preliminary and permanent injunctive relief is granted, Plaintiffs and the Class Members will suffer harm. Plaintiffs and the Class Members do not have an adequate remedy at law, and the balance of the equities weighs in favor of Plaintiffs and the Class Members.

150. At all material times, Defendant's deceptive trade practices were willful within the meaning of FDUTPA and, accordingly, Plaintiffs and the Class Members are entitled to an award of attorneys' fees, costs, and other recoverable expenses of litigation.

PRAYER FOR RELIEF

WHEREFORE, the representative Plaintiffs, on behalf of themselves and the plaintiffs who are described within the Rule 23 definition of any class certified by the Court, respectfully request that the Court:

A. certify this case as a class action pursuant to Fed. R. Civ. P. 23, appoint named-Plaintiffs as adequate Class representatives, and appoint Plaintiffs' undersigned counsel to represent the Class;

B. allow that, at the earliest possible time, Plaintiffs be allowed to give Notice of this action, or that the Court issue such Notice, to all persons who have, at any time up through and including the date of this Court's issuance of Court-supervised Notice, been employed, as described above, by Lincare. Such Notice shall inform such workers or former workers that this civil action has been filed and of the nature of the action;

C. find that Lincare breached its duties to safeguard and protect the PII of Plaintiffs and the Class Members that was compromised in the Data Breach;

D. declare unlawful the acts and practices alleged herein, and issue such injunctive and/or declaratory or other equitable relief to which the Plaintiffs may be entitled, so that Defendant's unlawful behavior may be stopped. Such injunctive relief may include, without limitation: (i) the provision of credit monitoring for at least 25 years, if not the remainder of the lives of Plaintiffs and the Class Members; (ii) the provision of bank

monitoring for at least 25 years, if not the remainder of the lives of Plaintiffs and the Class Members; (iii) the provision of internet monitoring; (iv) the provision of credit-restoration services for at least 25 years, if not the remainder of the lives of Plaintiffs and the Class Members; (v) the provision of identity-theft insurance for at least 25 years, if not the remainder of the lives of Plaintiffs and the Class Members; (vi) prohibiting Lincare from continuing its above-described wrongful conduct including, without limitation, the unauthorized release and disclosure of its current and former employees' PII; (vii) requiring Lincare to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data-security processes, controls, policies, procedures, and protocols to safeguard and protect the PII entrusted to it; (viii) periodic compliance audits by a third-party to ensure that Lincare is properly safeguarding and protecting the PII in its possession, custody, and control, and (ix) clear and effective notice to Class Members about the serious risks posed by the theft of PII and the precise steps that must be taken to protect themselves;

E. award Plaintiffs and the Class Members appropriate relief, including actual, statutory, and compensatory damages, as well as restitution and disgorgement, as a result of the wrongful and egregious acts complained of herein;

F. award equitable, injunctive, and/or declaratory relief, as appropriate;

G. award all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

H. grant incentive awards to the named Plaintiffs, as deemed reasonable by the Court;

I. award pre-judgment and post-judgment interest at the maximum rate allowed by law; and

J. grant any additional relief as the Court may find just and proper.

JURY DEMAND

Plaintiffs demand a trial by jury on all triable issues.

DATED: October 11, 2017

TRAGOS, SARTES & TRAGOS, PLLC

/s/Peter L. Tragos
PETER L. TRAGOS, ESQ.

601 Cleveland St., Suite 800
Clearwater, FL 33755
Telephone: (727) 441-9030
Facsimile: (727) 441-9254
Florida Bar No.: 0106744
Email: PeterTragos@greeklaw.com
Linda@greeklaw.com

JOHNSON FISTEL, LLP
Michael I. Fistel, Jr.
David A. Weisz
40 Powder Springs Street
Marietta, GA 30064
Telephone: (770) 200-3104
Facsimile: (770) 200-3101
Email: MichaelF@johnsonfistel.com
DavidW@johnsonfistel.com

JOHNSON FISTEL, LLP
Frank J. Johnson
Phong L. Tran
600 West Broadway, Suite 1540
San Diego, CA 92101
Telephone: (619) 230-0063
Facsimile: (619) 255-1856
Email: FrankJ@johnsonfistel.com
PhongT@johnsonfistel.com

Counsel for Plaintiffs

JS 44 (Rev. 11/15)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

ANDREW GIANCOLA, RAYMOND T. SCOTT, and PATRICIA SMITH, Individually and On Behalf of All Others Similarly Situated,

(b) County of Residence of First Listed Plaintiff Pinellas County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
TRAGOS, SARTES & TRAGOS, PLLC
Peter L. Tragos, 601 Cleveland St., Suite 800, Clearwater, FL 33755
Tel: (727) 441-9030, Fax: (727) 441-9254

DEFENDANTS

LINCARE HOLDINGS, INC.,

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	❒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	☒ 4
Citizen of Another State	❒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ❒ 110 Insurance
- ❒ 120 Marine
- ❒ 130 Miller Act
- ❒ 140 Negotiable Instrument
- ❒ 150 Recovery of Overpayment & Enforcement of Judgment
- ❒ 151 Medicare Act
- ❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ❒ 153 Recovery of Overpayment of Veteran's Benefits
- ❒ 160 Stockholders' Suits
- ❒ 190 Other Contract
- ❒ 195 Contract Product Liability
- ❒ 196 Franchise

REAL PROPERTY
- ❒ 210 Land Condemnation
- ❒ 220 Foreclosure
- ❒ 230 Rent Lease & Ejectment
- ❒ 240 Torts to Land
- ❒ 245 Tort Product Liability
- ❒ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ❒ 310 Airplane
- ❒ 315 Airplane Product Liability
- ❒ 320 Assault, Libel & Slander
- ❒ 330 Federal Employers' Liability
- ❒ 340 Marine
- ❒ 345 Marine Product Liability
- ❒ 350 Motor Vehicle
- ❒ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ❒ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ❒ 365 Personal Injury - Product Liability
- ❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ❒ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ❒ 370 Other Fraud
- ❒ 371 Truth in Lending
- ❒ 380 Other Personal Property Damage
- ❒ 385 Property Damage Product Liability

CIVIL RIGHTS
- ❒ 440 Other Civil Rights
- ❒ 441 Voting
- ❒ 442 Employment
- ❒ 443 Housing/ Accommodations
- ❒ 445 Amer. w/Disabilities - Employment
- ❒ 446 Amer. w/Disabilities - Other
- ❒ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ❒ 463 Alien Detainee
- ❒ 510 Motions to Vacate Sentence
- ❒ 530 General
- ❒ 535 Death Penalty

Other:
- ❒ 540 Mandamus & Other
- ❒ 550 Civil Rights
- ❒ 555 Prison Condition
- ❒ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ❒ 625 Drug Related Seizure of Property 21 USC 881
- ❒ 690 Other

LABOR
- ❒ 710 Fair Labor Standards Act
- ❒ 720 Labor/Management Relations
- ❒ 740 Railway Labor Act
- ❒ 751 Family and Medical Leave Act
- ❒ 790 Other Labor Litigation
- ❒ 791 Employee Retirement Income Security Act

IMMIGRATION
- ❒ 462 Naturalization Application
- ❒ 465 Other Immigration Actions

BANKRUPTCY
- ❒ 422 Appeal 28 USC 158
- ❒ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ❒ 820 Copyrights
- ❒ 830 Patent
- ❒ 840 Trademark

SOCIAL SECURITY
- ❒ 861 HIA (1395ff)
- ❒ 862 Black Lung (923)
- ❒ 863 DIWC/DIWW (405(g))
- ❒ 864 SSID Title XVI
- ❒ 865 RSI (405(g))

FEDERAL TAX SUITS
- ❒ 870 Taxes (U.S. Plaintiff or Defendant)
- ❒ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ❒ 375 False Claims Act
- ❒ 376 Qui Tam (31 USC 3729(a))
- ❒ 400 State Reapportionment
- ❒ 410 Antitrust
- ❒ 430 Banks and Banking
- ❒ 450 Commerce
- ❒ 460 Deportation
- ❒ 470 Racketeer Influenced and Corrupt Organizations
- ❒ 480 Consumer Credit
- ❒ 490 Cable/Sat TV
- ❒ 850 Securities/Commodities/ Exchange
- ❒ 890 Other Statutory Actions
- ❒ 891 Agricultural Acts
- ❒ 893 Environmental Matters
- ❒ 895 Freedom of Information Act
- ❒ 896 Arbitration
- ❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ❒ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d).

Brief description of cause:
Negligence, Breach of Fiduciary Duty & Implied Contract, Violation of Fl. Deceptive and Unfair Trade Practices Act

VII. REQUESTED IN COMPLAINT:

❒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
10/11/2017

SIGNATURE OF ATTORNEY OF RECORD
s/ Peter L. Tragos

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.