David H. Miller (Admitted Pro Hac Vice)
dmiller@sawayalaw.com
Adam M. Harrison (Admitted Pro Hac Vice)
aharrison@sawayalaw.com
THE SAWAYA & MILLER LAW FIRM
1600 Ogden Street
Denver, Colorado 80218
Phone: (303) 839-1650 x 1090
Fax: (303) 832-7102
Attorneys for Plaintiffs Price, Wilson and Esposito, on behalf of themselves and all others similarly situated

Scott B. Cooper (Admitted Pro Hac Vice)
Scott@cooper-firm.com
Samantha A. Smith (Admitted Pro Hac Vice)
samantha@cooper-firm.com
THE COOPER LAW FIRM, P.C.
4000 Barranca Parkway, Suite 250
Irvine, California 92604
Phone: (949) 724-9200
Fax: (949) 724-9255
Attorneys for Plaintiffs Hernandez, Byrne and Butler, on behalf of themselves and all others similarly situated

Jessica L. Campbell (Admitted Pro Hac Vice)
jcampbell@aegislawfirm.com
AEGIS LAW FIRM, PC
9811 Irvine Center Drive, Suite 100
Irvine, California 92618
Phone: (949) 379-6250
Fax: (949) 379-6251
Attorneys for Plaintiffs Beverly Porras and Leticia Stocks, on behalf of themselves and all others similarly situated

Graham S.P. Hollis (Admitted Pro Hac Vice)
ghollis@grahamhollis.com
Nicole R. Roysdon (Admitted Pro Hac Vice)
nroysdon@grahamhollis.com
GRAHAMHOLLIS, APC
3555 Fifth Avenue, Suite 200
San Diego, California 92103
Phone: (619) 692-0800
Fax: (619) 692-0822

Attorneys for Plaintiff Nancy Castellano,
on behalf of herself and all others similarly situated

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

IN RE: Sprouts Farmers Market, Inc. Employee Data Security Breach Litigation This Document Relates to: All Actions	MDL Docket No. 16-2731 HON. DOUGLAS L. RAYES **MASTER CLASS AND COLLECTIVE ACTION COMPLAINT AND JURY DEMAND**

MASTER COMPLAINT

Plaintiffs, Debra Price, Sean Wilson, Sandra Esposito, Julio Hernandez, Cynthia Byrne, Danielle Butler, Beverly Porras, Leticia Stocks, and Nancy Castellano (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their undersigned attorneys, as their Master Class and Collective Action Complaint against Defendants, Sprouts Farmers Market, Inc., SFM, LLC and SF Markets, LLC (collectively, "Sprouts" or "Defendants") hereby complain and allege as follows:

CLASS AND COLLECTIVE ACTION

This case is brought by Plaintiffs who had their personal identifying information

("PII") accessed, stolen, and used without their authorization, and who, because of the negligence, breaches of statutory, common law and contractual duties, and other acts and omissions described herein on the part of Defendants, suffered actual harm and monetary damages. Plaintiffs bring this action to obtain declaratory and injunctive relief, damages (including compensatory, statutory, exemplary and punitive damages), penalties, costs of suit, attorneys' fees and other appropriate relief on their own individual behalf, and on behalf of all others similarly situated, specifically, the more than 21,000 employees who worked for Sprouts during 2015. The case is brought as both a class and collective action, as described herein (hereinafter referred to as a "Class action").

NATURE OF THE CASE

1. Plaintiffs bring this case as a class and collective action on their own behalves and on the behalf of more than 21,000 employees who have had their PII and tax information accessed, stolen and used illegally as a result of the acts and failures to act of the Defendants. This case seeks to remedy the harmful effects of the data breach that occurred in or about March 2016, Defendants' failure to timely and reasonably notify Plaintiffs and the Class ("Plaintiffs") of the breach in accordance with the laws of most states, including Arizona and California, failure to abide by other laws that required that Plaintiffs' PII be secured, and, the insufficient remedy afforded by Defendants.

2. Defendants were negligent in storing, maintaining and disclosing their employees' 2015 IRS Form W-2s and that negligence has damaged and additionally placed Plaintiffs at an increased risk of fraud, identity theft, and financial injury associated with repairing the identity theft that has already occurred, monitoring future attempts at identity

theft, compensating the Plaintiffs for damage that has already occurred and will continue to occur in the future, and guarding against unauthorized tax filing and other abuse that is a direct and proximate result of Sprouts' violations of Plaintiffs' rights.

3. Defendants' current and former employees' most sensitive data, including over 21,000 Form W-2s and their related information (which includes social security numbers), was compiled and negligently released by Defendants in response to a "phishing scam" and is now in the possession of unknown third parties who are believed to be using the data for illegal purposes.

4. Defendants owed a legal duty to Plaintiffs and any and all employees who work or worked at a Sprouts location in California affected by the breach ("California Subclass Members") to maintain, protect, and safeguard their tax information. Defendants breached that duty by negligently compiling Plaintiffs' and California Subclass Members' private tax information and sending it off to third parties.

5. As a result of Defendants' failure to protect Plaintiffs' PII, Plaintiffs' and the other Class Members' private tax information and social security numbers were compromised, placing them at an increased risk of fraud and identity theft, and causing direct financial expenses, including time expended, associated with credit monitoring, replacement of compromised credit, debit and bank card numbers, and other measures needed to protect against the misuse of their private tax information.

JURISDICTION AND VENUE

6. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d). Plaintiffs and Defendants are residents of

different states. Sprouts is an incorporated for-profit business entity whose principal place of business and corporate headquarters is located in Phoenix, Arizona.

7. More than 21,000 Plaintiff Class Members nationwide had their PII accessed, wrongfully disclosed by Sprouts, and taken by unknown third parties. The aggregate amount in controversy exceeds $5,000,000.00.

8. This Court has personal jurisdiction over the parties because Defendants conduct substantial business in Arizona, have had systematic and continuous contacts within Arizona, and have agents and representatives that can be found in this State.

9. Under 28 U.S.C. § 1391, venue is proper in this District because Defendants engaged in substantial conduct relevant to the claims of Plaintiffs, and caused harm to Members of the Class, in this District.

PARTIES

10. Plaintiff Debra Price ("Price") is a former employee of Sprouts. Sprouts employed Price from approximately February 28, 2010 until approximately December 3, 2015. She worked as a courtesy clerk and then as a part time cashier. Price's PII was compromised when on or around March 14, 2016, a Sprouts employee who was given access to all of Plaintiffs' PII e-mailed complete copies of all current and former employees' 2015 IRS W-2 forms to a phishing scammer who pretended to be another Sprouts employee. After Price's W-2 was stolen, her identity was compromised. Price and her husband were unable to e-file their taxes because someone in possession of Price's social security number had already claimed a rapid refund through unknown sources to obtain Price's tax refund. Price has suffered actual, tangible damages. She will need to

expend additional time, money and resources to work with the IRS, her CPA, the State of Colorado and all credit reporting agencies to sort out the fraudulent tax claim made with her social security number that was compromised due to Sprouts' negligence and failure to protect her form W-2.

11. Plaintiff Sean Wilson ("Wilson") has been employed at Sprouts for approximately four (4) years in California. He has worked at two (2) California Sprouts stores; store numbers 249 and 228. He is currently the 3rd Supervisor in the Produce Department of store 228 located in San Diego, California. Like all other Class Members, Wilson's W2 information was stolen and used by an unknown person, and as a proximate result he will suffer and/or has suffered economic damages and other harm such as identity theft, and identity or medical fraud and has incurred and/or will incur costs associated with additional credit monitoring beyond the inadequate one-year monitoring offered by Sprouts. The theft and use of his personal information has caused actual and ongoing damage.

12. Plaintiff Sandra Esposito ("Esposito") was an employee of Sprouts in Scottsdale, Arizona during 2015 who worked as a salad clerk. In early April 2016, Esposito and her husband attempted to electronically file their taxes, but received an IRS notice that a return had already been filed for her social security number and she would not receive her refund until she followed IRS fraud procedures. Esposito has suffered actual, tangible damages. Most critically, she has been unable to obtain the refund that was expected and needed to pay for critical medical care. As of the filing of this Complaint, Esposito still has not received her tax return, but has put the family behind in billing schedules, causing

them to incur late fees. She will need to expend additional time, money and resources, to work with the IRS, her CPA, the State of Arizona and all credit reporting agencies to sort out the fraudulent tax claim made with her social security number that was compromised due to Sprouts' negligence and failure to protect her form W-2.

13. Plaintiff Julio Hernandez ("Hernandez") is a resident of the State of California who worked for Sprouts in San Diego, California. Sprouts employed Hernandez from approximately December, 2013 to February, 2016. To protect himself following the Data Breach, Hernandez signed up for identity theft protection through his bank, Wells Fargo, for $12.99 per month in addition to the one year credit monitoring offered by Defendants through Experian. To date, Hernandez has heard nothing from Defendants about the breach other than a form letter dated March 28, 2016, which was sent out to the employees.

14. Plaintiff Cynthia Byrne ("Byrne") is a resident of the State of California who is currently employed by Sprouts in San Diego, California. Byrne has been employed with Sprouts since approximately November, 1990. Since the Data Breach, Byrne has had her identity stolen when a tax return was filed using her name and social security number. Byrne has also started to receive harassing phone calls from people purporting to be from the IRS. Byrne has signed up for the one year credit monitoring offered by Defendants through Experian.

15. Plaintiff Danielle Butler ("Butler") is a resident of the State of New Hampshire and a former employee of Sprouts. Sprouts employed Ms. Butler at their corporate office in Phoenix, Arizona, from approximately May, 2011 to December, 2015.

Butler has had her identity stolen since the Data Breach when a federal tax return had been filed using her name and social security number. Butler never received any notice from Sprouts regarding the Data Breach despite reaching out to them several times. Butler learned about the Data Breach only after receiving a letter from the IRS regarding the fraud and hearing about the Data Breach from former coworkers. Butler has signed up for credit monitoring to protect herself against any future fraud.

16. Plaintiffs Beverly Porras ("Porras") and Leticia Stock ("Stock") are residents of California who were employed by Defendants during the relevant time period. Porras' and Stock's personal and financial information was compromised as a result of the Data Breach. Porras and Stock have suffered and continue to suffer economic injuries, anxiety, and stress as a result of the Data Breach. After receiving notice of the Data Breach, Porras and Stock enrolled in Experian credit monitoring either the same day they received notification or soon thereafter. Porras and Stock suffered loss of their time spent enrolling in credit monitoring and reviewing the credit reports received from that monitoring service. Porras suffered financial losses as a result of the Data Breach when she spent money to place a security freeze on her credit. Stock will suffer financial losses as a result of the Data Breach from buying fraud alert services. Stock has received multiple phone calls purporting to offer services related to credit cards and/or credit reporting. She had not received this high volume of calls in the past.

17. Plaintiff Nancy Castellano ("Castellano") is a resident of California who worked for Sprouts in La Jolla, California. Sprouts employed Castellano from approximately April 2015 to April 2016. She had her sensitive, non-public information,

including her social security number, compromised due to the W-2 Data Breach and has been injured as a result. Castellano has expended time and resources monitoring her credit for fraudulent activity, including signing up for a credit monitoring service and pulling and reviewing her credit report, and inquiring with the IRS about possible tax return fraud. Castellano never received formal notification of the W-2 Data Breach from Sprouts, other than the posting on the employee bulletin board at work.

18. Defendants Sprouts Farmers Market, Inc., SFM, LLC, and SF Markets, LLC (collectively, "Sprouts" or "Defendants") are entities organized under the laws of Delaware, with principal offices located in Phoenix, Arizona. As of January 25, 2016, Defendants were operating 224 stores in 13 states, including California. At all times relevant to this Complaint, Sprouts employed more than 21,000 people.

FACTUAL ALLEGATIONS

19. Plaintiffs hereby incorporate the preceding factual allegations as though fully set forth herein.

20. Sprouts owns and operates a chain of grocery stores throughout the United States.

21. Approximately 92 of Sprouts' stores are located in California, where Sprouts employs thousands of employees.

22. Plaintiffs and all Members of their Class ("Class Members"), were employed by Sprouts during the 2015 tax year.

23. Sprouts collects and stores their employees' Personal and Financial Information, including full names, social security numbers ("SSN"), wages, withheld

taxes, and addresses, which are included on Form W-2s for distribution to employees and tax authorities.

A. Sprouts' Data Breach

24. On March 14, 2016, an employee working in Sprouts' corporate payroll department received an e-mail purporting to be from a Sprouts senior executive. In this e-mail, the purported senior executive requested that the payroll employee send him or her the 2015 Form W-2 Wage and Tax Statements ("W-2s") for all employees who had worked for Sprouts in 2015. The Sprouts payroll employee compiled the requested W-2s and complied with the request by e-mailing the requested W-2s to the purported Sprouts senior executive (the "W-2 Data Breach").

25. Thereafter, on March 17, 2016, Sprouts discovered that the e-mail from the purported Sprouts senior executive was actually a "whaling" scam and that the payroll employee had improperly disclosed the unencrypted W-2s of over 21,000 Sprouts employees to an unauthorized third party. As a result, Sprouts released and disclosed Plaintiffs' and Class Members' PII, including their names, addresses, Social Security numbers, wages, and withheld taxes to an unauthorized third party and, potentially, the public.

26. A "whaling" scam is a variation of a "phishing" scam. A "phishing" scam is an attempt to acquire information, such as usernames, passwords, credit card details, and other sensitive or personal information, by masquerading as a trustworthy entity through an electronic communication, such as e-mail. A "whaling" scam 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 through an e-mail.

27. During tax season, cybercriminals most often use such phishing or whaling attacks to steal W-2 data to perform tax refund fraud; however, they also sell the information underground or use it to stage further attacks.

28. At all times relevant to this Complaint, Sprouts was advised by skilled lawyers, employees and other professionals who were knowledgeable about protection and storage of PII and the requirements of Arizona and California law.

29. Sprouts knew, or should have known, that it was susceptible to such attacks as various retailers, banks and hospitals have been hit recently in similar attacks, including a data breach experienced by Sprouts between January 25 and January 29, 2013 on their point of sale system that affected credit card terminals at 19 of Sprouts' 151 stores.

30. In the information age, such attacks are commonplace and Sprouts knew or should have known that fact and taken precautions to prevent becoming unwitting accomplices to the scam, especially in light of their point of sale data breach just a few years earlier.

31. Between March 1, 2016 and March 13, 2016, the following companies publicized similar data breaches that had occurred in February 2016 and March 2016 and in which employees' W-2 information was compromised and disclosed as a result of a "whaling" e-mail scam: Seagate Technology, Snapchat, Central Concrete Supply Co., Main Line Health, Turner Construction Company, Billy Casper Golf, Evening Post Industries, Information Innovators, Inc., York Hospital, Acronis, Money Tree, General

Communications, Inc., Advance Auto Parts, Applied Systems, Inc., eClinicalWorks, LAZ Parking, Endologix, Inc., ConvaTec, Inc., Care.com, Foss Manufacturing Company, Mitchell International, Inc., and Matrix Service Company. Based on these breaches, Sprouts knew or should have known that it was susceptible to such an attack.

32. Sprouts also ignored several warnings from the IRS regarding the prevalence in 2016 of malicious "phishing" e-mails being sent to individuals and companies to steal personal information.

33. On February 18, 2016, about a month before Sprouts' Data Breach, 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, who then uses the information for a variety of illegal activities, such as filing false tax returns to fraudulently obtain tax refunds.

34. On March 1, 2016, about two weeks before the Sprouts W-2 Data Breach, the IRS issued a public advisory warning to payroll and Human Resources 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 human resources 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 Personal and Financial Information, to cybercriminals posing as company executives. The IRS statement warned companies to check out e-mails that appear to come from high-ranking company executives, such as the CEO, 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.

35. Despite all of these warnings, Sprouts made no efforts to train their payroll department employees to avoid these scams.

36. The risk of theft by or disclosure to cyber criminals of sensitive data, including PII, stored electronically is well-known and common knowledge.

37. Despite this knowledge, Sprouts did not encrypt or password-protect any of the Plaintiffs' PII that it wrongfully disclosed.

38. Sprouts not only failed to take any precautions to prevent this attack, but have subsequently failed to make any appropriate efforts to remedy it.

B. Sprouts' Inadequate Response to the Data Breach

39. On March 17, 2016, Sprouts became aware of the Data Breach disclosing its employees' 2015 W-2s.

40. On or about March 18, 2016, Sprouts informally notified its employees about the W-2 Data Breach via e-mail and by posting the information on the employee bulletin board at its stores. See Exhibit A.

41. Castellano did not receive any notification via e-mail and was not aware of the W-2 Data Breach until she was advised to review the posting on the employee bulletin board at work on or about March 21, 2016. Sprouts' informal notification did not provide all of the details of the breach nor did it provide the information on how Plaintiffs could sign up for the free credit monitoring that Sprouts claimed it was offering. Instead, Plaintiffs and Class Members had to wait another ten days for the formal notification in order to obtain this information and protect themselves. The informal notification also did not confirm that all of Sprouts' employees who worked for the company in 2015 had been affected, but rather misled Plaintiffs and Class Members into believing that their PII may have only potentially been compromised.

42. On March 28, 2016, Sprouts mailed a letter to Plaintiffs, informing Plaintiffs that they and 21,000 of their former coworkers' 2015 W-2s were disclosed to an unknown person claiming to be a Sprouts senior executive. The letter stated that:

(a) Sprouts was the victim of a phishing scam the week of March 14, 2016;

(b) Sprouts disclosed all 2015 form W-2 wage and tax statements when fulfilling what was believed to be a legitimate request for information;

(c) Sprouts became aware of the incident on March 17, 2016;

(d) Sprouts disclosed the Form W-2s, which includes full name, address, SSN, wages, taxes withheld in 2015;

(e) Sprouts claimed that it did not disclose birthdate, bank information, credit card information, or e-mail addresses;

(f) Sprouts stated that they had taken steps to address the situation, and suggested steps the recipient of the letter could take to protect their personal information;

(g) Sprouts claimed they took immediate action as soon as they discovered the breach;

(h) Sprouts stated it contacted the FBI;

(i) Sprouts also stated that it communicated with their employees/former employees so that those employees and former employees could take steps to protect themselves;

(j) Sprouts offered each employee/former employee a complimentary one-year Membership of Experian's Protect MyID Alert;

(k) Sprouts suggested that each employee obtain their free credit report from the credit bureaus, and look to the FTC to obtain more information about placing a security freeze on their credit files, and placing a fraud alert on their accounts also;

(l) Sprouts set up a toll free hotline for questions – 855-814-8016 and teammemberhelp@sprouts.com.

43. The letter was signed by Brandon Lombardi, Chief Legal Officer.

44. Sprouts offered current and former employees twelve months of credit monitoring and insurance through Experian's ProtectMyID Alert. But credit monitoring

and insurance cannot prevent identity theft or fraud, even for over a twelve-month 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.

45. Sites ranking companies that provide identity protection services have noted that while many of these companies do offer services to prevent identity theft and fraud, ProtectMyID's services (ranked just 29th overall) focus more on credit monitoring rather than a more balanced and comprehensive approach to protection. Specifically, ProtectMyID lacks an analytical system (such as ID Analytics) that can search the dark web and protect private information, and provide real time alerts to victims when their identity has been compromised.

46. The letter Sprouts sent to Plaintiffs on March 28, 2016 squarely placed the burden on Plaintiffs and the Class Members, rather than Sprouts, to protect themselves and mitigate the damages flowing from the W-2 Data Breach – such as spending time reviewing their account statements and monitoring their credit reports. Unfortunately, many of Sprouts' mitigation directives require Plaintiffs and 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 California, the fee to place (and remove) a "security freeze" on one's credit report, as suggested by the W-2 Data Breach Notification, is approximately $10 each time it is placed at each of the three credit reporting agencies (Experian, Equifax, and Transunion). Monitoring one's credit reports, another option suggested by the W-2 Data Breach Notification, would cause a W-2 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. Sprouts has not offered to pay for the cost of these protections; however, York Hospital, which suffered a similar data breach only a few weeks before Sprouts, has offered to reimburse its employees for these costs for one year.

47. The PII "protection" offered by Sprouts is woefully inadequate because the free credit monitoring and identity theft insurance is only for one year. As advised by the Federal Trade Commission, a person impacted by a data breach should take proactive steps well after a year has passed to protect against identity theft and related fraud. The reason is that cybercriminals are aware that one year is the common duration for credit monitoring following a data breach and so they may wait until that year of credit monitoring is up before using the stolen PII for fraudulent means or selling it on the black market.

48. Further, Sprouts did not provide any protection against medical identity theft and fraudulent health insurance claims, the victims of which are often left with huge medical bills, damaged credit, and erroneous medical records.

49. Additionally, after Plaintiffs and 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 Sprouts decided not to provide or a continuation of the short program that Sprouts did offer. These advertisements will serve to further exploit Plaintiffs and Class Members.

50. Due to Sprouts' wrongful actions, inaction, omissions, and want of ordinary care, and the resulting W-2 Data Breach, Plaintiffs and Class Members have been and will be required to take affirmative steps to recover their peace of mind, and personal security, for which there is a financial and temporal cost. Plaintiffs and 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, (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 attempting to sort out issues related to the W-2 Data Breach, (vii) and even obtaining new Social Security numbers. However, Sprouts has not offered to pay Plaintiffs and Class Members for the time they have spent and will spend taking these actions.

51. Because Plaintiffs and Class Members have been required to take these actions as a result of their employment with Sprouts, and Sprouts is or should be aware that Plaintiffs and Class Members are taking such actions, and spending hours of their time to do so, Sprouts has suffered and permitted them to work and, thus, is required to pay them

at least minimum wage for all hours they spend taking such actions and provide them with accurate itemized wage statements reflecting the hours worked and wages earned.

52. Sprouts' wrongful actions, inaction, omissions, and want of ordinary care in failing to completely and accurately notify Plaintiffs and Class Members about the W-2 Data Breach and corresponding unauthorized release and disclosure of their PII were arbitrary, capricious and in derogation of Sprouts' duties to Plaintiffs and Class Members, and the notification procedures required by various state laws.

53. Even in the face of the IRS' warnings, the recent publicized similar W-2 data breaches, and the 2013 data breach of Sprouts' customers' credit card information, Sprouts did nothing to implement adequate security measures to detect and prevent a breach and disclosure of its employees' W-2s and PII.

C. The Gravity of the Data Breach

54. A person's social security number is perhaps the most important piece of information to an individual in the modern world. It is used, among other things, to verify eligibility for employment, to apply for a passport, to open a bank account, to apply for a credit card, or a student loan, or a 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.

55. The theft of Social Security numbers in particular, as opposed to other PII, is difficult to rectify because Social Security numbers are difficult to change and their misuse can continue for years into the future.

56. Identity thieves use Social Security numbers to commit other types of fraud, such as obtaining false identification cards, obtaining government benefits in the victim's name, committing crimes, and filing fraudulent tax returns to obtain tax refunds. Identity thieves also obtain jobs using compromised Social Security numbers, rent houses and apartments, and obtain medical services in the victim's name. Identity thieves may also give a victim's PII to police during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an unwarranted criminal record.

57. The unauthorized disclosure of a persons' 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.

58. 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.

59. Sprouts, as an employer, required Plaintiffs to surrender to it their SSNs and other PII, and Sprouts was entrusted with properly holding and safeguarding such PII.

60. Sprouts had a duty as an employer to guard and protect the private, highly sensitive, confidential PII of Plaintiffs and the Class Members.

61. Sprouts not only failed to safeguard and prevent the theft of this PII from its computers or network, but voluntarily handed it over to third parties upon their mere electronically-delivered e-mail request.

62. Sprouts failed to take reasonable precautions to protect the Plaintiffs' PII, and otherwise failed to act reasonably in fulfillment of their duty not to disclose Plaintiffs' PII, and affirmatively to protect that PII.

63. Sprouts negligently and carelessly kept its employees' and former employees' personal information.

64. Sprouts did not encrypt or password-protect Plaintiffs' social security numbers as a prudent and responsible company would do with its employees' confidential and personal identifying information.

65. Sprouts 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 the Plaintiffs' personal, and financial PII and failed to retain this PII in a secure and safe manner.

66. Arizona's Consumer Protection Act prohibits a person or entity from requiring an individual to transmit his or her social security number over the internet, unless the connection is secure or the social security number is encrypted.

67. Cal. Civ. Code §1798.81.5 requires any business that maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access or disclosure.

68. Sprouts violated California law by failing to implement reasonable or appropriate security procedures, measures or protocols to protect its current and former employees' PII in accordance with the law.

69. As a direct and proximate result of Sprouts' actions, all its 2015 employees and former employees have been required to spend man hours addressing and ameliorating or otherwise dealing with actual and ongoing harm to the PII and W2 information – information that Sprouts would not have been able to wrongfully disclose but for the employment relationship between it and the Plaintiffs. Thus, Sprouts has failed to pay the Plaintiffs and Class at least minimum wage for the time spent as a result of its actions.

70. Within only a week of the W-2 Data Breach, Plaintiffs' PII was used to steal Plaintiffs' federal tax returns, to wreak havoc on Plaintiffs' tax filings and to cause unmeasured damage to the Plaintiffs' identities, which damage is ongoing.

71. The number of workers affected is believed to be over 21,000.

D. The Preventability of the Data Breach

72. Sprouts 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 Sprouts did nothing to expand, improve, or update them.

73. Although Sprouts could not have prevented the phishing e-mail from being sent, the W-2 Data Breach could have been prevented or greatly minimized had Sprouts utilized the proper data security measures, processes, controls, policies, procedures, and protocols. Sprouts recognized as much as it asserted in its W-2 Data Breach Notification that it was working to enhance its controls and make additional investments in protocols, technology, and training. See Exhibit B.

74. The W-2 Data Breach could have been prevented had Sprouts implemented securely configured mail services with advanced spam filters so that the phishing e-mail never reached the payroll employee's inbox in the first place.

75. The W-2 Data Breach could have been prevented had Sprouts conducted information security training throughout the company. Sprouts should have provided education and training to its payroll and Human Resources employees, as well as any other employees with access to employee 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; (v) and

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 have a "need to know" for the data requested.

76. The W-2 Data Breach also could have been prevented had Sprouts implemented data security controls, policies, and procedures regarding payroll and Human Resources employees' access to employee PII. Sprouts should have had policies in place that prohibited payroll and Human Resources employees from having on-demand access to all of its employees' PII or at least required payroll and Human Resources employees to go through multiple layers of computer system security and scrutiny, such as requiring approval from a superior or involving the information technology or security team, before being provided access to so much sensitive information at one time.

77. The W-2 Data Breach could have been prevented had Sprouts implemented data security measures to ensure that employee PII was never sent in an unencrypted form. Sprouts 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, Sprouts should have implemented a data security measure that provided it with the capability to remotely delete a file that was mistakenly sent.

78. Had Sprouts taken even these most fundamental data security measures, the W-2 Data Breach never would have happened.

E. The Harms Suffered by Plaintiffs

79. During the week of April 4, 2016, Price's CPA attempted to e-file Price and her husband's joint tax return for 2015 with the IRS. However, the return was rejected because Price's SSN had already been used by an unknown person to get a rapid refund.

80. On April 8, 2016, Price called the IRS to alert them of the apparent theft of her SSN and her tax refund. The IRS confirmed the SSN used was Price's and put an alert on the return. As of this date it is unknown exactly what process Price and her husband will be able to use to file their taxes. But it is clear that Price's SSN is compromised and will require additional time, money and effort to repair the damage already done, to ensure that her SSN is not used again and to do or undo whatever is necessary to repair the breach.

81. Price's minor daughter was also an employee of Sprouts during 2015 and her W-2 has also been compromised, leaving her vulnerable to identity theft and a threat that her credit will be compromised before she even has a chance to build that credit.

82. As a result of the data breach, unknown third parties now possess the PII of Sprouts' employees and former employees who are the Plaintiffs in this case.

83. As a direct and proximate effect of Sprouts' disclosure of its employees 2015 W-2s the Plaintiffs' SSNs were stolen and used to claim Price, Esposito and Wilson's tax refunds and an as yet unknown number of other Class Members' tax refunds.

84. Upon information and belief, the information was disseminated and transmitted over the internet in and from the state of Arizona by Sprouts.

85. To protect himself following the Data Breach, Hernandez signed up for identity theft protection through his bank, Wells Fargo, for $12.99 per month in addition

to the one year credit monitoring offered by Sprouts through Experian. To date, Hernandez has heard nothing from Sprouts about the breach other than the form letter dated March 28, 2016, which was sent out to the employees. He has already expended several hours attempting to safeguard himself from identity theft and other harms caused by the release of his Form W-2 related tax information and social security number. Going forward, Hernandez anticipates spending considerable time in an effort to contain the impact of Sprouts' Data Breach on himself.

86. Hernandez suffers from an increased risk of future identity theft as a result of Sprouts' actions. In addition to suffering loss of time enrolling in credit monitoring services and reviewing his credit, Hernandez has suffered financial losses as a result of signing up for additional credit protection through his bank.

87. Byrne received the form letter sent by Sprouts dated March 28, 2016. Unfortunately for Byrne, her identity has already been stolen and her social security number compromised. Byrne was contacted by the IRS by a letter dated April 20, 2016, informing her that a tax return was filed using her name and social security number and the IRS needed to verify her identity before processing the return. In a subsequent letter dated May 4, 2016, the IRS informed Byrne that someone attempted to impersonate her by using her name and social security number by filing a fraudulent tax return in her name. Byrne has also started to receive harassing phone calls from people purporting to be from the IRS. Byrne has signed up for the one year credit monitoring offered by Sprouts through Experian. Byrne has already expended several hours attempting to safeguard herself from identity theft and other harms caused by the release of her Form W-2 related tax

information and social security number. Going forward, Byrne anticipates spending considerable time in an effort to contain the impact of Sprouts' Data Breach on herself.

88. Byrne suffers from an increased risk of future identity theft as a result of Sprouts' actions. In addition to suffering loss of time enrolling in credit monitoring services and reviewing and monitoring her credit, Byrne has suffered, and continues to suffer, enormous stress over the theft of her identity.

89. Like Byrne, Butler has already had her identity stolen. Butler was contacted by the IRS by a letter dated April 20, 2016, informing her that that a federal tax return had been filed using her name and social security number. Butler never received any notice from Sprouts regarding the Data Breach despite reaching out to them several times. Butler learned about the Data Breach only after receiving the letter from the IRS and hearing about the Data Breach from former coworkers. Butler has already expended several hours attempting to safeguard herself from identity theft and other harms caused by the release of her Form W-2 related tax information and social security number. Going forward, Butler anticipates spending considerable time in an effort to contain the impact of Sprouts' Data Breach on herself.

90. Like all Plaintiffs and Members of the Class, Butler suffers from an increased risk of future identity theft as a result of Sprouts' actions. In addition to suffering loss of time enrolling in credit monitoring services and reviewing and monitoring her credit, Butler has suffered, and continues to suffer, enormous stress over the theft of her identity.

91. To protect herself following the Data Breach, Castellano signed up for a credit monitoring service, pulled and reviewed her credit report, and inquired with the IRS

about possible tax return fraud. To date, Castellano has not received formal notification of the W-2 Data Breach from Sprouts, other than the posting on the employee bulletin board at work, nor has she received any other communications from Sprouts regarding the Data Breach. Castellano has already expended time and resources attempting to safeguard herself from identity theft and other harms caused by the release of her Form W-2 related tax information and social security number. Going forward, Castellano anticipates spending additional time in an effort to contain the impact of Sprouts' Data Breach on herself. Castellano also suffers from an increased risk of future identity theft as a result of Sprouts' actions.

92. After receiving notice of the Data Breach, Porras and Stock enrolled in Experian credit monitoring either the same day they received notification or soon thereafter. Porras suffered financial losses as a result of the Data Breach when she spent money to place a security freeze on her credit. Stock will suffer financial losses as a result of the Data Breach from buying fraud alert services. Stock has received multiple phone calls purporting to offer services related to credit cards and/or credit reporting. Stock had not received this high volume of calls in the past.

93. Sprouts flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy rights, and harmed them in the process, by not obtaining their prior written consent to disclose their PII to any other person or entity – as required by California statutory and common laws.

94. Sprouts flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy 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 and, potentially, the public without their authorization.

95. Sprouts flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy 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 Class Members' PII. Sprouts' failure to do so – even in the face of previous similar W-2 data breaches in the weeks and months before at other companies and the IRS' warnings to beware of such breaches – is an abuse of discretion and confirms its intentional and willful failure to observe procedures required by law and industry standards and recommendations.

96. Sprouts flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy rights, and harmed them in the process, by failing to completely notify and inform them about the W-2 Data Breach and the disclosure of their PII in an expedient manner.

97. Sprouts' inadequate W-2 Data Breach Notification – including its failure to provide Plaintiffs and Class Members with adequate and reasonable protection or sufficient relief from the W-2 Data Breach – substantially increased Plaintiffs' and Class Members' imminent risk of identity theft, identity fraud, or medical fraud.

98. 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.

99. Sprouts flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy 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.

100. As a direct and proximate result of Sprouts' above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting W-2 Data Breach, Plaintiffs and Class Members have incurred (and will continue to incur) economic damages and other injury and actual harm, which harm is ongoing.

CLASS ACTION ALLEGATIONS

101. Plaintiffs hereby incorporate the preceding factual allegations as though fully set forth herein.

102. In addition to bringing this case individually, Plaintiffs also bring this case as a Class Action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of all Plaintiffs and as Members of the following proposed Class:

> **All current and former employees of Sprouts who worked at Sprouts and received a Form W-2 for work performed in 2015, and who, during the period beginning on or about March 14, 2016 and continuing through the present had their PII disclosed and disseminated by Sprouts to a third party.**

103. Plaintiffs also seek to certify a California Subclass consisting of all Members of the Class who are or were residents of California under the respective Data Breach statute of California. This Class is defined as follows:

> **All current and former employees of Sprouts who were residents of California as of March 14, 2016, and whose 2015 Form W-2s and related information were transmitted to a third party in or around the week of March 14, 2016.**

Numerosity

104. The proposed Class is so numerous that joinder of all of its Members is impractical. In excess of 21,000 current and former employees of Sprouts suffered the loss of their PII due to the actions and failures of Sprouts.

105. The putative Class Members are so numerous and dispersed throughout the United States that joinder of all Members is impracticable.

106. Putative Class Members can be identified by records maintained by Sprouts.

Common Questions of Law and Fact

107. Common questions of fact and law exist as to all Members of the Class and predominate over any questions affecting solely individual Members of the Class, pursuant to Rule 23(b)(3).

108. Among the questions of fact and law that predominate over any individual issues are:

a. Whether Sprouts received and stored PII of Plaintiffs and the Members of the Class;

b. The standard to which Sprouts is to be held with respect to its possession and/or dissemination of Plaintiffs' PII;

c. Whether Sprouts 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 Plaintiffs' and Class Members' PII that was disclosed without authorization in the W-2 Data Breach;

d. Whether Sprouts failed to act reasonably in protecting the PII of Plaintiffs in its care, custody and control;

e. Whether the actions and/or failures to act of Sprouts caused the PII of Plaintiffs and Class Members to be accessed, stolen and/or used without authorization;

f. Whether Sprouts failed to timely and reasonably notify Plaintiffs and Class Members of the theft of their PII in conformity with the laws of Arizona, California and other states;

g. Whether Sprouts was negligent;

h. Whether Sprouts' notification contained false or misleading information and/or failed to inform Plaintiffs and Class Members of material information necessary to allow Plaintiffs to protect themselves from further harm due to the disclosure of their PII;

i. Whether Sprouts' conduct with respect to the Data Breach was unfair and deceptive;

j. Whether Sprouts' conduct constituted unfair methods of competition and/or was unfair and/or unlawful;

k. Whether Sprouts has been unjustly enriched by having obtained the labor and other benefits from services of Plaintiffs and Class Members, and the saving of costs that would have been expended had they acted reasonably to protect the PII in their care, custody and control;

l. Whether Sprouts breached its agreements, express and implied, with Plaintiffs and Class Members;

m. Whether Sprouts violated a duty of good faith and fair dealing in its agreements with Plaintiffs and Class Members;

n. Whether Sprouts breached a fiduciary duty it had toward Plaintiffs and Class Members;

o. Whether Sprouts complied with the security notification laws of Arizona and other States upon learning of the breach of the PII of Plaintiffs and Class Members;

p. Whether Sprouts violated the consumer protection laws of Arizona and other states through their acts and omissions set forth in this Complaint;

q. Whether Plaintiffs and the Class Members are at an increased risk of identity theft as a result of Sprouts' breaches and failure to protect Plaintiffs' and the Class Members' private tax information and social security numbers;

r. Whether Sprouts unlawfully failed to inform Plaintiffs and Class Members that it did not maintain and implement data security measures, procedures,

and protocols adequate to reasonably safeguard employees' PII and whether Sprouts failed to inform Plaintiffs and Class Members of the W-2 Data Breach in a timely and accurate manner;

s. Whether the Plaintiffs and Members of the Class were "employees" under the Fair Labor Standards Act for work they reasonably had to perform to safeguard their PII because of the actions or inactions of Sprouts;

t. Whether Sprouts failed to pay Plaintiffs and Class Members at least minimum wage for the time they spent taking actions to protect themselves and deal with the ramifications of the W-2 Data Breach;

u. Whether Sprouts failed to provide Plaintiffs and Class Members with accurate itemized wage statements reflecting the hours worked and wages earned for time they have spent taking actions to protect themselves and deal with the ramifications of the W-2 Data Breach;

v. Whether Sprouts failed to indemnify Plaintiffs and Class Members for the losses and expenses they have suffered as a result of the W-2 Data Breach;

w. Whether Plaintiffs and Class Members suffered injury, including ascertainable losses, as a result of Sprouts' actions, inaction, omission, and want of ordinary care;

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

y. whether Plaintiff and Class members are entitled to recover penalties; and

z. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief.

Typicality

109. Plaintiffs' claims are typical of the claims of the Members of the Class. Plaintiffs and Class Members sustained injuries as a result of the unlawful disclosure of their PII, which injuries were directly and proximately caused by Sprouts' acts and omissions.

110. As detailed herein, Plaintiffs' known harms that have already occurred consisted of the actual theft of their identities by the use of their SSN to file fraudulent tax returns, which resulted in costs, expenses, emotional distress and other damages and is likely to cause additional and continuing damage to all Plaintiffs and Class Members.

Adequacy of Representation

111. Plaintiffs can and will fairly and adequately represent and protect the interests of the Class, and Plaintiffs have no interests that conflict with or are antagonistic to the interests of the Members of the Class.

112. Plaintiffs have retained competent attorneys with over 30 years of experience in complex Class actions, including employment related Class actions.

113. No conflict exists between Plaintiffs and the Members of the Class.

//

//

Superiority

114. A Class action is superior to any other available method for the fair and efficient adjudication of this controversy and common questions of law and fact overwhelmingly predominate over any individual questions that may arise.

115. The prosecution of separate actions by individual Members of the plaintiff Class would create a risk of inconsistent or varying adjudications with respect to individual Members of the Class. These adjudications would establish incompatible standards of conduct for Sprouts which would, as a practical matter, be disparities of the claims of the other Members not parties to the adjudications or substantially impair or impede their ability to protect their interests.

116. By its dissemination of the Plaintiffs' PII, Sprouts has acted or refused to act on grounds generally applicable to all Members of the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

Public Policy Considerations

117. Current employees are often afraid to assert their rights against their employers out of fear of direct or indirect retaliation. Former employees are fearful of bringing actions against their employers because they believe their former employers might damage their future endeavors through negative references and/or other means. Class actions provide the Class Members who are not named in the complaint with a type of anonymity that allows for the vindication of their rights at the same time as affording them privacy protections.

118. Accordingly, Class certification is appropriate under Rule 23 of the Federal Rules of Civil Procedure.

CALIFORNIA LABOR CODE PRIVATE ATTORNEYS GENERAL ACT ("PAGA") REPRESENTATIVE ACTION ALLEGATIONS.

119. Plaintiffs hereby incorporate the preceding factual allegations as though fully set forth herein.

120. The California claims alleged herein are appropriately suited for a Labor Code Private Attorneys General Act of 2004 ("PAGA") action because:

a. Pursuant to California Labor Code § 2699(a), any provision of the Labor Code "that provides for a civil penalty to be assessed and collected by the Labor and Workforce Development Agency or any of its departments, divisions, commissions, boards, agencies, or employees, for a violation of this code, may, as an alternative, be recovered through a civil action brought by an aggrieved employee on behalf of himself or herself and other current or former employees pursuant to the procedures specified in section 2699.3."

b. This action involves allegations of violations of provisions of the California Labor Code that provide or do not provide for a civil penalty to be assessed and collected by the Labor & Workforce Development Agency ("LWDA") or any departments, divisions, commissions, boards, agencies or employees;

c. Plaintiffs are "aggrieved employees" because they were employed by the alleged violators and had one or more of the alleged violations committed against them; and

d. On April 8, 2016, Castellano satisfied the procedural requirements of § 2699.3 by serving, via Certified Mail, the LWDA and her employers SPROUTS FARMERS MARKET, INC. and SFM, LLC with her notice for wage and hour violations and penalties, including the facts and theories to support each violation. More than 33 days have passed since Castellano served notice via Certified Mail to the LWDA and Sprouts. Therefore, Plaintiffs have satisfied all the administrative requirements to pursue civil penalties against Defendants pursuant to California Labor Code § 2698, et seq.

e. Castellano filed her action pursuant to Labor Code § 2699(a) and (f), on behalf of herself and all other current and former aggrieved employees of Sprouts to recover civil penalties. Said civil penalties include unpaid wages which are to be paid to the affected employees pursuant to Labor Code § 558 subdivisions (a)(1) and (a)(3).

f. Castellano's action was subsequently consolidated into this action.

g. Defendants were Plaintiffs' employers or persons acting on behalf of Plaintiffs' employers, within the meaning of California Labor Code § 558, who violated or caused to be violated, a section of Part 2, Chapter 1 of the California Labor Code or any provision regulating hours and days of work in any order of the Industrial Welfare Commission and, as such, are subject to penalties for each underpaid employee, as set forth in Labor Code § 558, at all relevant times.

h. Plaintiffs seek to recover all applicable civil penalties under PAGA on behalf of themselves and all other aggrieved employees including, but not limited to, all unpaid and/or underpaid wages pursuant to Labor Code § 558, Reynolds v. Bement, 36 Cal.4th 1075, 1089 (2005), and Thurman v. Bayshore Transit Management, Inc., 203 Cal. App. 4th 1112 (2012).

COUNT I:

NEGLIGENCE

121. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

122. Defendants owed a duty of care to Plaintiffs and the Class to ensure that their PII was not accessed or used for improper purposes. This duty included, among other things, designing, maintaining and testing Sprouts' security systems to ensure that Plaintiffs' and Class Members' private tax information and social security numbers in Sprouts' possession were adequately secured and protected. Sprouts further owed a duty to Plaintiffs and the Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warning and alerts including those generated by its own security systems.

123. Sprouts owed a duty to Plaintiffs and the Class Members to provide security, consistent with industry standards and requirements, to ensure that its systems and networks, and the personnel responsible for them, adequately protected the private tax information and social security numbers of its current and former employees.

124. Sprouts owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate security practices.

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

126. Sprouts also owed a duty to timely and accurately disclose to Plaintiffs and the Class Members that their private tax information and social security numbers had been or were reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and the Class Members could take appropriate measures to avoid identify theft or fraudulent charges, including, monitoring their account information and credit reports for fraudulent activity, contacting their banks or other financial institutions, obtaining credit monitoring services, filing reports with law enforcement and other governmental agencies and taking other steps to mitigate or ameliorate the damages caused by Sprouts' misconduct.

127. Sprouts' procedures for handling the financial and personal information of its current and former employees were intended to and did affect Plaintiffs and Class Members. Sprouts knew that by collecting and storing its employees' sensitive personal and financial information, it undertook a responsibility to take reasonable security measures to protect the information from being exposed to unauthorized persons.

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

the steps and opportunities to prevent and stop the Data Breach as set forth herein. Sprouts' 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.

129. Plaintiffs and the Class Members entrusted Sprouts with their private tax information and social security numbers with the understanding that Sprouts would safeguard their information and that the company was in a position to protect against the harm suffered by Plaintiffs and the Class Members as a result of the Data Breach.

130. Defendants breached their duty of care to Plaintiffs and the Class to ensure that their PII was not used for improper purposes by failing to provide adequate protections of the PII, by negligently disseminating the PII, and by allowing the PII to be accessed, in unencrypted format, by third parties.

131. Sprouts also breached its duties to timely and accurately disclose that Plaintiffs' and Class Members' private tax information and social security numbers in Sprouts' possession had been or was reasonably believed to have been, stolen or compromised.

132. As a direct and proximate result of Defendants' failure to take reasonable care and use at least industry-standard measures to protect the personal and financial information placed in their care, Plaintiffs and Class Members had their personal and financial information stolen, causing direct and measurable monetary losses, threat of future losses, identity theft and/or threat of identity theft.

133. As a direct and proximate result of Defendants' negligence and misconduct, Plaintiffs and Class Members were injured in fact or will be injured by actual harm in the form of: damage to credit scores and credit reports; heightened risk of identity theft; other fraudulent activity; and time and expense related to: (a) finding and contesting fraudulent activity; (b) finding and buying services to prevent identity theft and monitor their credit; (d) flagging assets and accounts for fraud; (e) reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (f) reviewing credit reports; (g) repairing damage to credit and other financial accounts; (h) the general stress and anxiety of dealing with all these issues resulting from the Data Breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Data Breach, all of which have an ascertainable monetary value to be proven at trial.

134. As a result of Sprouts' negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not necessarily 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 Sprouts for the purpose of deriving employment from Sprouts and with the understanding that Sprouts 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; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from 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 and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, which remains in Sprouts' possession and is subject to further breaches so long as Sprouts fails to undertake the implementation of appropriate and adequate security measures, procedures, and protocols 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 W-2 Data Breach for the remainder of the lives of Plaintiffs and Class Members.

135. Plaintiffs and the Class Members have spent time and money to protect themselves as a result of Defendants' conduct, and will continue to be required to spend time and money protecting themselves, their identities, their credit, and their reputations.

136. But for Sprouts' 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 Class Members would not have been injured, and Plaintiffs and Class Members would not be at a heightened risk of identity theft in the future.

137. Sprouts' negligence was a substantial factor in causing harm to Plaintiffs and Class Members. As a direct and proximate result of Sprouts' failure to exercise reasonable care and implement and maintain reasonable security measures, controls, procedures, and protocols, the PII of Sprouts' current and former employees was accessed by unauthorized individuals who may: (i) have already used the compromised information to commit identity theft and fraud; (ii) continue to use their compromised PII to commit identity theft and identity and health care and/or medical fraud; and (iii) post the information on the internet, allowing themselves and others to commit identity theft, and identity and health care and/or medical fraud using the compromised PII indefinitely.

138. As a direct and proximate result of Sprouts' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the W-2 Data Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm, which is ongoing.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT II:

VIOLATIONS OF THE ARIZONA CONSUMER FRAUD ACT

139. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

140. Sprouts engaged in an unfair or deceptive trade practice by not protecting and by not encrypting Plaintiffs' and the Class' PII when it transmitted its employees' social security numbers over the internet.

141. The lax security protocols and failure to encrypt Plaintiffs' and the Class' PII was a practice that occurred in the course of Defendants' business.

142. Defendants' failure to adequately protect the Plaintiffs and the Class' PII impacts its employees, who represent over 21,000 consumers who are also Members of the public and its actual or potential consumers of the Defendants' goods.

143. As a direct and proximate result of Defendants' unfair trade practices, Plaintiffs and Class Members suffered injury in fact to the protected interest of keeping their PII confidential and out of the hands of criminals and the practice caused the Plaintiffs actual injury

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT III:

BREACH OF FIDICUARY DUTY

144. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

145. Defendants were fiduciaries, as employers, required to act primarily for the benefit of Defendants' employees in matters connected with their employment.

146. Plaintiffs and the Class were in a fiduciary relationship by way of the duty Defendants had in relation to the employment of Plaintiffs, and Defendants' duty to act for or to give advice for the benefit of Plaintiffs and the Class 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.

147. Defendants breached their duty of care to Plaintiffs and the Class 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 third parties to whom Sprouts voluntarily disseminated the information.

148. As a direct and proximate result of the Defendants' actions alleged above, the Plaintiffs suffered actual damages.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT IV:

BREACH OF CONFIDENTIALITY

149. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

150. Plaintiffs' and Class Members' unique and private Personal and Financial Information in Defendants' possession, custody, and control was (and continues to be) highly confidential.

151. Defendants breached the confidentiality of Plaintiffs' and Class Members' Personal and Financial Information by failing to identify, implement, maintain, and monitor appropriate data security measures, policies, procedures, and protocols to ensure the security and confidentiality of Plaintiffs' and Class Members' Personal and Financial Information, and wrongfully releasing and disclosing their Personal and Financial Information without authorization, as described above.

152. Had Defendants not engaged in the above-described wrongful actions, inaction, and omissions, the Data Breach never would have occurred and Plaintiffs' and Class Members' Personal and Financial Information would not have been wrongfully released, disclosed, and compromised. Defendants' wrongful conduct constitutes (and continues to constitute) the tort of breach of confidentiality at common law.

153. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injuries and actual harm in the form of, inter alia: damage to credit scores and credit reports; heightened risk of identity theft; other fraudulent activity; and time and expense related to: (a) finding and contesting fraudulent activity; (b) finding and buying services to prevent identity theft and monitor their credit; (d) flagging assets and accounts for fraud; (e) reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (f) reviewing credit reports; (g) repairing damage to credit and other financial accounts; (h) the general stress and anxiety of dealing with all these issues resulting from the Data Breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Data Breach, all of which have an ascertainable monetary value to be proven at trial.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT V:

BREACH OF CONTRACT

154. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

155. Plaintiffs and the Members of the Class had employment agreements with Defendants. These agreements involved a mutual exchange of consideration whereby Defendants entrusted Plaintiffs and the Class to work in various roles (such as courtesy clerk and cashier in its grocery stores) on its behalf, in exchange for the promise of employment, with wages, benefits in some cases, and secure PII.

156. The failure of Defendants to keep secure from breach the PII of Plaintiffs and the Class constitutes a material breach of the agreement between the Defendants and the Class.

157. As a direct and proximate result of the aforesaid breaches of Defendants' agreements with Plaintiffs and the Class, Plaintiffs and the Class have been harmed.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT VI:

BREACH OF IMPLIED CONTRACT

158. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

159. Plaintiffs and the Class were required by Defendants to provide PII as a condition of their employment.

160. Implicit in the employment agreement between Defendants and Plaintiffs and Members of the Class was the obligation that both parties would maintain information confidentially and securely.

161. Defendants implicitly and/or explicitly promised to keep the PII they collected from Plaintiffs and the Class secure and confidential. In addition, Defendants implicitly promised to retain this PII only under conditions that safeguarded such information, and to either destroy it after the employment ended, or to take appropriate steps to ensure that it was not improperly lost or stolen.

162. Defendants had an implied duty of good faith to ensure that the Personal and Financial Information of Plaintiffs and Class Members in their possession was only used to provide the agreed-upon compensation and other employment benefits from Defendants. Defendants were therefore required to reasonably safeguard and protect the Personal and Financial Information of Plaintiffs and Class Members from unauthorized uses, and to timely and accurately notify Plaintiffs and Class Members if their Personal and Financial Information was compromised so that Plaintiffs and Class Members could act to mitigate the harm caused by the loss of opportunity to control how their Personal and Financial Information was used.

163. Plaintiffs and Class Members accepted Defendants' employment offer and fully performed their obligations under the implied contract with Defendants by providing their Personal and Financial Information to Defendants, among other obligations.

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

165. Defendants breached their implied contracts with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Personal and Financial Information and by failing to provide timely and accurate notice to Plaintiffs and Class Members that their Personal and Financial Information was compromised as a result of the Data Breach.

166. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injuries and actual harm in the form of, inter alia: damage to credit scores and credit reports; heightened risk of identity theft; other fraudulent activity; and time and expense related to: (a) finding and contesting fraudulent activity; (b) finding and buying services to prevent identity theft and monitor their credit; (d) flagging assets and accounts for fraud; (e) reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (f) reviewing credit reports; (g) repairing damage to credit and other financial accounts; (h) the general stress and anxiety of dealing with all these issues resulting from the Data Breach; and (g) costs associated with the loss of

productivity from taking time to ameliorate the actual and future consequences of the Data Breach, all of which have an ascertainable monetary value to be proven at trial.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT VII:

VIOLATION OF RIGHT TO PRIVACY/
PUBLIC DISCLOSURE OF PRIVATE FACTS

167. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

168. Plaintiffs and Class Members have a legally-protected privacy interest in their PII.

169. Plaintiffs and Class Members had a reasonable expectation of privacy in providing their PII to Defendants in the context of their employment with Defendants.

170. Defendants, through their negligence and carelessness, disclosed facts, specifically Plaintiffs' and the Class' PII, which are private in nature.

171. By failing to protect those private facts the PII was disclosed to an unknown person or persons on the internet.

172. Defendants' disclosure of Plaintiffs' and the Class' PII and the subsequent illicit use of that information was and is highly offensive to a reasonable person.

173. Plaintiffs' and the Class' W-2 information is not of legitimate concern to the public, and will only be used for nefarious purposes.

174. By not protecting Plaintiffs' and the Class' PII, including their W-2s, the Defendants acted with reckless disregard for the private nature of the facts that were disclosed.

175. As a direct and proximate result of Sprouts' actions and inactions the Plaintiffs have suffered, and will continue to suffer actual damages.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT VIII:

UNJUST ENRICHMENT

176. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

177. By their above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach – to wit, Defendants' failure to identify, implement, maintain, and monitor the proper data security measures, policies, procedures, and protocols to safeguard and protect Plaintiffs' and Class Members' Personal and Financial Information – Defendants have been (and continue to be) unjustly enriched by, inter alia: (i) the saved cost of implementing the proper Personal and Financial Information security measures, policies, procedures, and protocols in their corporate payroll department, that they did not implement, (ii) the shifted risk and expense of the Data Breach to Plaintiffs and Class Members, and (iii) the return on investment on all above-described amounts.

178. Defendants, therefore, should be compelled to refund (or disgorge) such wrongfully collected, saved back, and shifted funds and expenses under the common law equitable doctrine of unjust enrichment.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT IX:

FAILURE TO PAY MINIMUM WAGES AND OVERTIME IN VIOLATION OF THE FAIR LABOR STANDARDS ACT

29 U.S.C. § 201 et seq.

179. Pursuant to the applicable provisions of the Fair Labor Standards Act ("FLSA"), 29 U.S.C. § 206 and § 207, the named Plaintiffs and the Class similarly situated were entitled to at least the minimum hourly wage, for each hour that they labored in Defendants' business and, in the event they worked more than 40 hours a week, an overtime hourly wage of time and one-half such minimum hourly wage for all hours worked in excess of 40 hours per week.

180. Through Sprouts' wrongful conduct alleged herein, Sprouts suffered and permitted Plaintiffs and the Class Members to work and failed to pay them at least minimum wage for all of the time that Plaintiffs and the Class Members reasonably have spent to address and attempt to ameliorate, mitigate, and deal with the actual and ongoing consequences of its release of PII. That work suffered includes but is not limited to: (i) identifying and dealing with fraudulent charges and accounts, including tax refund fraud, (ii) frequently obtaining and/or purchasing credit reports from multiple credit reporting

agencies, (iii) placing and removing fraud alerts and security freezes on credit reports, (iv) obtaining and/or purchasing credit monitoring and internet monitoring services, (v) obtaining and/or purchasing identity theft insurance, (vi) spending time on the telephone attempting to sort out issues related to the breach, (vii) and in some instances obtaining new Social Security numbers.

181. Sprouts placed the burden on Plaintiffs and Class Members to spend hours of their time addressing these issues.

182. Plaintiffs and Class Members have been required to take these actions as a result of their employment with Sprouts, and Sprouts is or should be aware that Plaintiffs and Class Members are taking such actions, and spending hours of their time to do so.

183. Sprouts has suffered and permitted Plaintiffs to work and, thus, is required to pay them at least minimum wage for all hours they spend taking such actions.

184. As a direct result of Sprouts' conduct alleged herein, Plaintiffs and Class Members have suffered and continue to suffer, substantial losses related to the use and enjoyment of such wages.

185. Plaintiffs seek to recover in a civil action the unpaid balance of the full amount of the unpaid wages resulting from Sprouts' minimum wage violations including interest thereon, reasonable attorney's fees and costs of suit, and liquidated damages to the fullest extent permissible.

186. The Plaintiffs and the Class were paid no monetary compensation whatsoever by Defendants for performing labor suffered or permitted by Defendants and arising from the employer/employee relationship and such failure to pay the Plaintiffs and

the Class any compensation whatsoever violates the minimum hourly wage requirements of 29 U.S.C. § 206 and, in the event any of the Class Members or Plaintiffs ever worked in excess of 40 hours in a week, the overtime pay requirements of 29 U.S.C. § 207.

187. Plaintiffs, on behalf of themselves and all other similarly situated persons who consent in writing to join this action, it also being proposed that all such persons be notified of this action through the dispatch of a written notice to the last known names and addresses of such persons that are set forth in the Defendant's records or that can otherwise be ascertained, seek, on this Claim for Relief, a judgment for unpaid minimum wages and overtime wages and additional liquidated damages of 100% of any such unpaid wages, such sums to be determined based upon an accounting of the hours worked by the named Plaintiffs and any such other persons who consent to join this action, and the Plaintiffs also seek an award of attorney's fees, interest and costs as provided for by the FLSA.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the Class, respectfully seek the relief set forth below.

COUNT X:

FAILURE TO PAY MINIMUM WAGES IN VIOLATION OF CALIFORNIA LAW

Cal. Lab. Code §§ 1194, 1197, 1198, IWC Wage Order 7-2001

California Subclass

188. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

189. Plaintiffs and California Subclass Members are/were "non-exempt" employees of Sprouts in California within the meaning of the Labor Code and IWC Wage Order 7-2001 and all other applicable state laws.

190. California Labor Code section 1197 states: "The minimum wage for employees fixed by the commission is the minimum wage to be paid to employees, and the payment of a less wage than minimum wage so fixed is unlawful."

191. Labor Code section 1197.1 states: "Any employer or other person acting either individually or as an officer, agent, or employee of another person, who pays or causes to be paid to any employee a wage less than the minimum fixed by an order of the commission shall be subject to a civil penalty, restitution of wages, liquidated damages payable to the employee, and any applicable penalties imposed pursuant to Section 203. For any initial violation that is intentionally committed, one hundred dollars ($100) for each underpaid employee for each pay period for which the employee is underpaid. For each subsequent violation for the same specific offense, two hundred fifty dollars ($250) for each underpaid employee for each pay period for which the employee is underpaid regardless of whether the initial violation is intentionally committed."

192. Labor Code section 1198 states: "The maximum hours of work and the standard conditions of labor fixed by the commission shall be the maximum hours of work and the standard conditions of labor for employees. The employment of any employee for longer hours than those fixed by the order or under conditions of labor prohibited by the order is unlawful."

193. IWC Wage Order 7-2001 section 4 provides that an employer may not pay employees less than the applicable minimum wage for all hours worked.

194. Through Sprouts' wrongful conduct alleged herein, Sprouts violated California Labor Code sections 1197, 1198 and the applicable IWC Wage Order when it suffered and permitted Plaintiffs and California Subclass Members to work and failed to pay them at least minimum wage for all of the time that Plaintiffs and California Subclass Members have spent to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the W-2 Data Breach, including, but not limited to: (i) identifying and dealing with fraudulent charges and accounts, including tax refund fraud, (ii) frequently obtaining and/or purchasing credit reports from multiple credit reporting agencies, (iii) placing and removing fraud alerts and security freezes on credit reports, (iv) obtaining and/or purchasing credit monitoring and internet monitoring services, (v) obtaining and/or purchasing identity theft insurance, (vi) spending time on the telephone attempting to sort out issues related to the W-2 Data Breach, (vii) and even obtaining new Social Security numbers.

195. Sprouts has placed the burden on Plaintiffs and California Subclass Members to spend hours of their time addressing these issues; however, because Plaintiffs and California Subclass Members have been required to take these actions as a result of their employment with Sprouts, and Sprouts is or should be aware that Plaintiffs and California Subclass Members are taking such actions, and spending hours of their time to do so, Sprouts has suffered and permitted them to work and, thus, is required to pay them at least minimum wage for all hours they spend taking such actions.

196. Labor Code section 1194 states: "Notwithstanding any agreement to work for a lesser wage, any employee receiving less than the legal minimum wage or the legal overtime compensation applicable to the employee is entitled to recover in a civil action the unpaid balance of the full amount of his minimum wage or overtime compensation, including interest thereon, reasonable attorney's fees and costs of suit." Labor Code section 1194.2 states: "In any action under Section 98, 1193.6, 1194, or 1197.1 to recover wages because of the payment of a wage less than the minimum wage fixed by an order of the commission or by statute, an employee shall be entitled to recover liquidated damages in an amount equal to the wages unlawfully unpaid and interest thereon."

197. As a direct result of Sprouts' conduct alleged herein, Plaintiffs and California Subclass Members have suffered and continue to suffer, substantial losses related to the use and enjoyment of such wages, including lost interest on such monies and expenses and attorney's fees in seeking to compel Sprouts to fully perform its obligations under state law, all to their respective damage in amounts according to proof at trial and within the jurisdictional limitations of this Court.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the California Subclass, respectfully seek the relief set forth below.

//

//

//

COUNT XI:

VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT

Cal. Civ. Code §1798.80, *et seq*.

California Subclass

198. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

199. "[T]o ensure that personal information about California residents is protected," the California Legislature enacted Civil Code section 1798.81.5, which requires that any business that "owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

200. Sprouts is a "business" within the meaning of Civil Code section 1798.80(a).

201. Each member of the California Subclass is an "individual" as defined by Civil Code section 1798.80(d).

202. The employee information taken in the Data Breach was "personal information" as defined by Civil Code sections 1798.80(e) and 1798.81.5(d), which includes "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card

number, debit card number, or any other financial information, medical information, or health insurance information."

203. The unauthorized acquisition of Plaintiffs' and the California Subclass Members' private tax information and social security numbers constituted a "breach of the security system" of Sprouts.

204. Sprouts unreasonably delayed informing anyone about the breach of security of California Subclass Members' confidential and non-public information after Sprouts knew the Data Breach had occurred.

205. Upon information and belief, no law enforcement agency instructed Sprouts that notification to California Subclass Members would impede its investigation.

206. Pursuant to Section 1798.84 of the California Civil Code:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

207. By failing to implement reasonable security measures, procedures, and protocols appropriate to the nature of the personal information of their current and former employees, Defendants violated Cal. Civ. Code §1798.81.5.

208. In addition, by failing to immediately notify all affected current and former Defendants employees that their personal information had been acquired (or was

reasonably believed to have been acquired) by unauthorized persons in the Data Breach, Defendants violated Cal. Civ. Code §1798.82 of the same title.

209. Defendants' failure to immediately notify employees of the breach caused Plaintiffs and California Subclass Members to suffer damages because they have lost the opportunity to immediately take mitigating action, including but not limited to: (a) finding and contesting fraudulent activity; (b) finding and buying services to prevent identity theft and monitor their credit; (d) flagging assets and accounts for fraud; (e) reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (f) reviewing credit reports; (g) repairing damage to credit and other financial accounts; (h) avoiding the general stress and anxiety of dealing with all these issues resulting from the Data Breach; and (g) losing productivity from taking time to ameliorate the actual and future consequences of the Data Breach.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the California Subclass, respectfully seek the relief set forth below.

COUNT XII:

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200 *et seq*.

California Subclass

210. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

211. California Business & Professions Code § 17200 prohibits any "unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."

212. Defendants' conduct, as alleged herein, has been and continues to be unfair, unlawful and harmful to Plaintiffs and California Subclass Members.

213. Plaintiffs seek to enforce important rights affecting the public interest within the meaning of Code of Civil Procedure § 1021.5.

214. A violation of Business and Professions Code §§ 17200, et seq. may be predicated on the violation of any state or federal law.

215. Defendants violated the Unfair Competition Law ("UCL") by intentionally accepting and storing Plaintiffs' and the California Subclass Members' personal and financial information but failing to take reasonable steps to protect it.

216. In violation of industry standards and best practices, Defendants also violated Plaintiffs' and the California Subclass Members' reasonable expectations that they would safeguard Personal and Financial Information, thereby creating for Defendants an artificially lower cost of doing business in order to undercut their competitors and establish and gain a greater foothold in the marketplace.

217. Defendants also violated the UCL by intentionally failing to immediately notify Plaintiffs and the California Subclass of the Data Breach. If Plaintiffs and the California Subclass had been notified in an appropriate fashion, they could have taken precautions to better safeguard their Personal and Financial Information.

218. In the course of conducting their business, Defendants committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, and protocols to safeguard and protect Plaintiffs' and California Subclass Members' Personal and Financial Information – especially in light of Sprouts' 2013 data breach, the prior W-2 data breaches that other companies had experienced in the weeks and months leading up to the Data Breach, and the warnings from the IRS to be aware of phishing scam e-mails seeking employee W-2s – violating the statutory and common laws alleged herein in the process, including, inter alia, the California Customer Records Act.

219. Plaintiffs and California Subclass Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

220. Sprouts had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of the private tax information and social security numbers of Plaintiffs and the California Subclass Members.

221. Sprouts also had exclusive knowledge about the extent of the Data Breach, including during the days and weeks following the Data Breach.

222. Sprouts also had exclusive knowledge about the length of time that it maintained former employees' private tax information and social security numbers after they left Sprouts' employment.

223. Sprouts failed to disclose, and actively concealed, the material information it had regarding Sprouts' deficient security policies and practices, and regarding the security of the private tax information and social security numbers of Plaintiffs and the California Subclass Members.

224. Sprouts' omissions were material, misleading, and had a tendency to deceive.

225. Plaintiffs were misled by Sprouts' omissions about Sprouts' data security, and reasonably relied upon them to their detriment.

226. But for Sprouts' omissions, Plaintiffs would have insisted that their private tax information and social security number be more securely protected, and Plaintiffs would have asked that their private tax information and social security numbers be removed from Sprouts' systems promptly after their employment ended. They also would have taken additional steps to protect their identities and to protect themselves from the sort of harm that could flow from Sprouts' lax security measures.

227. But for Sprouts' omissions, Plaintiffs would not be experiencing the increased risk of harm they are now facing as a result of the Data Breach, and could have taken more immediate measures to prevent potential harm.

228. Sprouts' above-described wrongful actions, inaction, omissions, want of ordinary care, and practices, also constitute "unfair" business acts and practices in violation of the UCL in that Sprouts' wrongful conduct is substantially injurious to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous.

229. The gravity of Sprouts' wrongful conduct outweighs any alleged benefits attributable to such conduct.

230. Moreover, there were reasonably available alternatives to further Sprouts' legitimate business interests other than engaging in the above-described wrongful conduct.

231. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiffs and California Subclass Members have suffered (and will continue to suffer) economic damages and other injuries and actual harm in the form of, inter alia: damage to credit scores and credit reports; heightened risk of identity theft; other fraudulent activity; and time and expense related to: (a) finding and contesting fraudulent activity; (b) finding and buying services to prevent identity theft and monitor their credit; (d) flagging assets and accounts for fraud; (e) reporting the theft of their social security numbers to financial institutions, credit agencies, and the IRS; (f) reviewing credit reports; (g) repairing damage to credit and other financial accounts; (h) the general stress and anxiety of dealing with all these issues resulting from the Data Breach; and (g) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Data Breach, all of which would have been unnecessary but for Defendants' conduct.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the California Subclass, respectfully seek the relief set forth below.

//

//

//

COUNT XIII:

INDEMNIFICATION

Cal. Lab. Code §§ 2800 and 2802

California Subclass

232. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

233. Under California Labor Code § 2800, an employer must indemnify its current and former employees for losses caused by the employer's want of ordinary care.

234. Under California Labor Code § 2802, an employer also must indemnify its current and former employees for all necessary expenditures or losses incurred by the employees in directly discharging their duties, or in obedience to the employer's directions, even though unlawful, unless the employee, at the time of his or her obedience, believed them to be lawful.

235. Sprouts required its current and former employees, including Plaintiffs and California Subclass Members, to provide their confidential and personal PII as a condition of employment. Sprouts, however, failed to safeguard and protect their PII by failing to identify, implement, maintain, and monitor appropriate data security measures, policies, procedures, and protocols which, in turn, directly and proximately caused the W-2 Data Breach, and Sprouts' unauthorized release and disclosure of their PII to an unauthorized third party.

236. As a direct and proximate result of Sprouts' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused

the W-2 Data Breach, and violation of the California Labor Code, Plaintiffs and California Subclass Members have suffered (and will continue to suffer) economic damages and other injury and actual harm, which harm is ongoing.

237. Sprouts has intentionally and willfully failed and refused to reimburse Plaintiffs and California Subclass Members for such losses and expenses. Plaintiffs and California Subclass Members, therefore, are entitled to recover such losses and expenses incurred during the course and scope of their employment, plus attorneys' fees, litigation expenses, costs, and interest under Cal. Lab. Code §§ 2800 and 2802.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the California Subclass, respectfully seek the relief set forth below.

COUNT XIV:

FAILURE TO PROVIDE ACCURATE ITEMIZED WAGE STATEMENTS IN VIOLATION OF CALIFORNIA LAW

Cal. Lab. Code § 226, IWC Wage Order 7-2001

California Subclass

238. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

239. California Subclass Members are employees of Sprouts in California within the meaning of the Labor Code and the applicable IWC Wage Order.

240. Labor Code section 226(a) states in pertinent part:

> Every employer shall, semimonthly or at the time of each payment of wages, furnish each of his or her employees, either as a detachable part of the check, draft, or voucher paying the employee's wages, or

separately when wages are paid by personal check or cash, an accurate itemized statement in writing showing:

(1) Gross wages earned;

(2) Total hours worked by the employee, except for any employee whose compensation is solely based on a salary and who is exempt from payment of overtime under subdivision (a) of Section 515 or any applicable order of the Industrial Welfare Commission;

(3) The number of piece-rate units earned and any applicable piece rate if the employee is paid on a piece-rate basis;

(4) All deductions, provided that all deductions made on written orders of the employee may be aggregated and shown as one item;

(5) Net wages earned;

(6) The inclusive dates of the period for which the employee is paid;

(7) The name of the employee and only the last four digits of his or her social security number or an employee identification number other than a social security number;

(8) The name and address of the legal entity that is the employer; and

(9) All applicable hourly rates in effect during the pay period and the corresponding number of hours worked at each hourly rate by the employee.

The deductions made from payment of wages shall be recorded in ink or other indelible form, properly dated, showing the month, day, and year, and a copy of the statement and the record of the deductions shall be kept on file by the employer for at least three years at the place of employment or at a central location within the State of California.

241. IWC Wage Order 7-2001 section 7(A) states in relevant part that the employer shall keep accurate information regarding, "(4) Total wages paid each payroll

period, including value of board, lodging, or other compensation actually furnished to the employee; (5) Total hours worked in the payroll period and applicable rates of pay."

242. Through Sprouts' conduct alleged herein, including but not limited to, Sprouts' failure to pay California Subclass Members at least minimum wage for all of the time they have spent to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the W-2 Data Breach, Sprouts failed to provide California Subclass Members with accurate itemized wage statements including, but not limited to, the recording of all time worked, all wages earned, and the applicable rates of pay for time worked.

243. California Subclass Members suffered injuries as a result of Sprouts' intentional and knowing failure to provide to Plaintiffs and California Subclass Members and maintain the writings required by Labor Code section 226(a). Sprouts' failure to provide and maintain accurate wage statements left California Subclass Members without the ability to know, understand and question the hours worked and wages earned and due. As a direct result, California Subclass Members have suffered and continue to suffer substantial injuries, losses and actual damages related to Sprouts' conduct, including lost wages, lost interest on such wages, and expenses and attorney's fees in seeking to compel Sprouts to fully perform its obligations.

244. Labor Code § 226(e) states: "An employee suffering injury as a result of a knowing and intentional failure by an employer to comply with subdivision (a) is entitled to recover the greater of all actual damages or fifty dollars ($50) for the initial pay period in which a violation occurs and one hundred dollars ($100) per employee for each violation

in a subsequent pay period, not exceeding an aggregate penalty of four thousand dollars ($4,000), and is entitled to an award of costs and reasonable attorney's fees."

245. Labor Code § 226(e)(2)(B) states "An employee is deemed to suffer injury for purposes of this subdivision if the employer fails to provide accurate and complete information as required by any one or more of items (1) to (9), inclusive, of subdivision (a) and the employee cannot promptly and easily determine from the wage statement alone one or more of the following: (i) The amount of gross wages or net wages paid to the employee during the pay period or any other information required to be provided on the itemized wage statement pursuant to items (2) to (4), inclusive, (6) and (9) of subdivision (a)…"

246. Because California Subclass Members' wage statements did not include an accurate accounting of the time spent to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the W-2 Data Breach, and, thus, among other things, the gross wages earned or total hours worked, they are deemed to have suffered injury.

247. Labor Code § 226(h) states "An employee may also bring an action for injunctive relief to ensure compliance with this section, and is entitled to an award of costs and reasonable attorney's fees."

248. As a direct result of Sprouts' conduct alleged herein, Plaintiffs and California Subclass Members have suffered and continue to suffer injury including substantial losses related to the use and enjoyment of such wages, lost interest on such monies and expenses and attorney's fees in seeking to compel Sprouts to fully perform its obligations under state

law, all to their respective damage in amounts according to proof at trial and within the jurisdictional limitations of this Court.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the California Subclass, respectfully seek the relief set forth below.

COUNT XV:

REPRESENTATIVE CLAIMS UNDER THE CALIFORNIA LABOR CODE PRIVATE ATTORNEYS GENERAL ACT

Cal. Lab. Code § 2698 et seq.

California Subclass

249. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

250. Pursuant to California Labor Code § 2699(a), any provision of the Labor Code that provides for a civil penalty to be assessed and collected by the LWDA or any of its departments, divisions, commissions, boards, agencies or employees for violation of the code may, as an alternative, be recovered through a civil action brought by an aggrieved employee on behalf of himself or herself and other current or former employees pursuant to the procedures specified in Labor Code § 2699.3.

251. This action involves allegations of violations of Labor Code §§ 226, 226.3, 558, 1194, 1194.2, 1197, 1197.1, 1198, 2800, and 2802 that pursuant to Labor Code § 2699.5 provide for a civil penalty to be assessed and collected by the LWDA or recovered through a civil action brought by an aggrieved employee on behalf of himself or herself

and other current or former employees pursuant to the procedures specified in Labor Code § 2699.3.

252. Pursuant to Labor Code § 2699(a), Castellano seeks civil penalties on behalf of herself and all other current and former employees of Defendants who reside or have resided in California and whose PII was compromised as a result of the W-2 Data Breach publicized in March 2016.

253. Sprouts employed Castellano and she had one or more of the alleged violations committed against her. Therefore, Castellano is an "aggrieved employee" under PAGA because the alleged violator employed her and she had one or more of the alleged violations committed against her. As such, Castellano is properly suited to represent the interests of other current and former aggrieved employees in a PAGA Representative action.

254. On April 8, 2016, pursuant to Labor Code §§ 2698, et seq., Castellano served, via Certified Mail, the LWDA and her employers SPROUTS FARMERS MARKET, INC. and SFM, LLC with her claim for wage/hour violations and penalties. More than 33 days have passed since Castellano served notice via Certified Mail to the LWDA and her employers. Therefore, Plaintiffs satisfied all the administrative requirements to pursue civil penalties against SPROUTS FARMERS MARKET, INC. and SFM, LLC pursuant to Labor Code §§ 2698, et seq.

255. Sprouts violated Labor Code §§ 1194 and 1197 by not paying Plaintiffs and aggrieved employees at least minimum wages for all the time they were suffered or permitted to work. Plaintiffs and the aggrieved employees have spent time taking actions

to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the W-2 Data Breach. Sprouts has not compensated them in any way for this time that they have expended in the course and scope of their employment as a result of Sprouts' disclosure of their PII in the W-2 Data Breach. Thus, under Labor Code § 2699(f)(2), Sprouts is subject to a civil penalty of $100 for each aggrieved employee per pay period for the initial violation of these sections, and $200 for each aggrieved employee per pay period for each subsequent violation.

256. Sprouts violated Labor Code §§ 2800 and 2802 by failing to indemnify Plaintiffs and the aggrieved employees for the losses and expenses that they incurred in the discharge of their job duties and that were caused by Sprouts' want of ordinary care. Sprouts has failed to indemnify Plaintiffs and the aggrieved employees for the losses and expenses that they have suffered as a result of the W-2 Data Breach, which were incurred in the course and scope of their employment. Thus, under Labor Code § 2699(f)(2), Sprouts is subject to a civil penalty of $100 for each aggrieved employee per pay period for the initial violation of these sections, and $200 for each aggrieved employee per pay period for each subsequent violation.

257. Sprouts violated Labor Code § 226(a) by failing to pay Plaintiffs and the aggrieved employees at least minimum wage for all of the time they have spent to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the W-2 Data Breach, and, thus, failing to provide Plaintiffs and aggrieved employees with accurate itemized wage statements including, but not limited to, the recording of all time worked, all wages earned, and the applicable rates of pay for time worked. Thus, under

Labor Code § 2699(f)(2), Sprouts is subject to a civil penalty of $100 for each aggrieved employee per pay period for the initial violation of this section, and $200 for each aggrieved employee per pay period for each subsequent violation.

258. Labor Code § 226.3 provides for a civil penalty in the amount of $250 per violation in an initial citation and $1,000 for each violation in a subsequent citation, for which the employer fails to provide the employee a wage deduction statement or fails to keep the records required in subdivision (a) of § 226.

259. For all provisions of the Labor Code for which a civil penalty is not specifically provided, Labor Code § 2699(f) imposes upon Defendants a penalty of one hundred dollars ($100.00) for each aggrieved employee per pay period for the initial violation and two hundred dollars ($200.00) for each aggrieved employee per pay period for each subsequent violation.

260. Sprouts is and was Plaintiff's and aggrieved employees' employer or other person(s) acting either individually or as an officer, agent, or employee of another person(s), who pays or causes to be paid to any employee a wage less than the minimum fixed by an order of the Commission, and, as such, is subject to penalties for each underpaid employee pursuant to Labor Code § 1197.1.

261. Labor Code § 1197.1 imposes upon Sprouts for each initial violation of wage and hour laws a penalty of $100.00 for each underpaid employee for each pay period for which the employee is underpaid. This amount shall be in addition to an amount sufficient to recover underpaid wages and liquidated damages pursuant to § 1194.2.

262. Furthermore, Labor Code § 1197.1 imposes upon Sprouts for each subsequent violation of wage and hour laws a penalty of $250.00 for each underpaid employee for each pay period for which the employee was underpaid in addition to an amount sufficient to recover the underpaid wages and liquidated damages pursuant to § 1194.2.

263. Sprouts is and was Plaintiff's and other aggrieved employees' employers, or persons acting on their behalf, within the meaning of Labor Code § 558, who violated or caused to be violated, a section of Part 2, Chapter 1 of the Labor Code or any provision regulating hours and days of work in any IWC Wage Order and, as such, is subject to penalties for each underpaid employee as set forth in Labor Code § 558.

264. Pursuant to Labor Code § 558 and Labor Code § 2699(a) and (f), Sprouts is subject to a civil penalty of $50.00 for an initial violation of any provision regulating the hours and days of work in any IWC Wage Order, for each aggrieved employee, for each pay period for which the aggrieved employee was not provided with all minimum wages for all hours suffered and permitted to work, as alleged herein. The civil penalty is in addition to an amount sufficient to recover the underpaid minimum wages, which shall be paid directly to each affected employee.

265. Furthermore, Labor Code § 558 imposes upon Sprouts for each subsequent violation of any provision regulating the hours and days of work in any IWC Wage Order a penalty of $100.00 for each aggrieved employee for each pay period for which the aggrieved employee was not provided with all minimum wages for all hours suffered and permitted to work, as alleged herein. The civil penalty is in addition to an amount sufficient

to recover the underpaid minimum wages, which shall be paid directly to each affected employee.

266. Sprouts violated Labor Code § 1198 when it failed to comply with the maximum hours of work and the standard conditions of labor fixed by the IWC under the "Hours and Days of Work" and the "Records" Sections of the applicable Wage Order, by failing to pay all minimum wages and failing to provide accurate itemized wage statements, as alleged herein. Thus, under Labor Code § 2699(f)(2), Sprouts is subject to a civil penalty of $100 for each aggrieved employee per pay period for the initial violation of Labor Code § 1198 and $200 for each aggrieved employee per pay period for each subsequent violation of Labor Code § 1198.

267. For bringing this action, Plaintiffs are additionally entitled to attorney's fees and costs incurred herein.

268. Plaintiffs seek to recover civil penalties on behalf of themselves and other aggrieved employees for Sprouts' violations of the Labor Code, including but not limited to Sprouts' violations of Labor Code §§ 226, 226.3, 558, 1194, 1194.2, 1197, 1197.1, 1198, 2800, and 2802 pursuant to Labor Code §§ 2698, et seq. The exact amount of the applicable penalty is an amount to be shown according to proof at trial.

WHEREFORE, Plaintiffs, on behalf of themselves and the aggrieved employees, respectfully seek the relief set forth below.

//

COUNT XVI:

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT

Cal. Civ. Code §§ 56, *et seq.*

California Subclass

269. Plaintiffs incorporate by reference the preceding and following paragraphs as though fully set forth herein.

270. Section 56.10 of the California Civil Code provides that "[a] provider of health care, health care service plan, or contractor shall not disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care plan without first obtaining an authorization."

271. Pursuant to Cal. Civ. Code § 56.05(j), "medical information" is any individually identifiable information that "includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, …, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity."

272. At all relevant times, Sprouts was both a contractor and a health care provider because it had the "purpose of maintaining medical information … in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his or her information, or for the diagnosis or treatment of the individual." Cal. Civ. Code § 56.06(a).

273. At all relevant times, Sprouts collected, stored, managed, and transmitted Plaintiffs' and California Subclass Members' PII in order to provide health insurance and workers' compensation benefits and facilitate health insurance and workers' compensation claims.

274. The CMIA requires Sprouts to implement and maintain standards of confidentiality with respect to all PII disclosed to it, and maintained by it. Specifically, Cal. Civ. Code § 56.10(a) prohibits Sprouts from disclosing Plaintiffs' and California Subclass Members' PII without first obtaining their authorization to do so.

275. Section 56.11 of the California Civil Code specifies the manner in which authorization must be obtained before PII is released. Sprouts, however, failed to obtain the proper authorization – much less, any authorization – from Plaintiffs and California Subclass Members before releasing and disclosing their PII. Sprouts also failed to identify, implement, maintain and monitor the proper data security measures, policies, procedures, and protocols to safeguard and protect Plaintiffs' and California Subclass Members' PII as required by California law. As a direct and proximate result of Sprouts' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and California Subclass Members' PII was wrongfully released and disclosed to an unauthorized third party. By disclosing Plaintiffs' and California Subclass Members' PII without their written authorization, Sprouts violated California Civil Code §§ 56, et seq., and its legal duty to protect the confidentiality of such information.

276. Sprouts also violated sections 56.06 and 56.101 of the California CMIA, which prohibits the negligent creation, maintenance, preservation, storage, abandonment,

destruction, or disposal of confidential PII. As a direct and proximate result of Sprouts' wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the W-2 Data Breach, Plaintiffs' and California Subclass Members' confidential PII was wrongfully released and disclosed without their authorization.

277. As a direct and proximate result of Sprouts' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the W-2 Data Breach, and violation of the CMIA, Plaintiffs and California Subclass Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) actual identity theft, identity fraud, or medical fraud, (ii) breach of implied contract, (iii) invasion of privacy, (iv) breach of the confidentiality of their PII, (v) statutory nominal damages of $1,000 per Plaintiff and each Class member under the CMIA (Cal. Civ. Code § 56.36(b)(1)), (vi) unpaid minimum wages and liquidated damages (Cal. Lab. Code §§ 1194, 1197, 1198), (vii) inaccurate wage statements (Cal. Lab. Code § 226), (viii) expenses and losses in discharging their duties (Cal. Lab. Code §§ 2800 and 2802), (ix) deprivation of the value of their PII, for which there is a national and international market, (x) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (xi) the imminent, immediate, and continuing increased risk of identity theft, identity fraud, or medical fraud – for which they are entitled to compensation.

278. As a direct and proximate result of Sprouts' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the W-2 Data Breach and its violation of the CMIA, Plaintiffs and California Subclass

Members also are entitled to: (i) injunctive relief, (ii) punitive damages of up to $3,000 per Plaintiff and each Class member, and (iii) attorneys' fees, litigation expenses and court costs under Cal. Civ. Code § 56.35.

WHEREFORE, Plaintiffs, on behalf of themselves and the Members of the California Subclass, respectfully seek the relief set forth below.

PRAYER FOR RELIEF

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

A. Certify this case as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, and as a collective action under the FLSA, and denominate Plaintiffs as adequate representatives for the Class and the undersigned counsel as counsel for the Class and collective action;

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 Sprouts. Such Notice shall inform such workers or former workers that this civil action has been filed and of the nature of the action;

C. 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 the unlawful behavior of the Defendants may be

stopped. Such injunctive relief may include, without limitation: (i) the provision of credit monitoring for at least 25 years; (ii) the provision of bank monitoring for at least 25 years; (iii) the provision of internet monitoring; (iv) the provision of credit restoration services for at least 25 years; (v) the provision of identity theft insurance for at least 25 years; (vi) prohibiting Sprouts from continuing its above-described wrongful conduct including, without limitation, the unauthorized release and disclosure of its current and former employees' PII; (vii) requiring Sprouts 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 Sprouts 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;

D. Award the actual, statutory and compensatory damages incurred by Plaintiffs and the Members of the Class as a result of the wrongful acts complained of herein, along with pre-judgment and post- judgment interest at the maximum rate allowed by law;

E. Award Plaintiffs and Class Members their unpaid wages and overtime compensation, along with liquidated damages in an amount equal to the wages and/or overtime compensation awarded;

F. Award statutory nominal damages of $1,000 per California Subclass Member under the CMIA (Cal. Civ. Code § 56.36(b)(1));

G. Award Plaintiffs punitive, exemplary and special damages for the wanton and willful behavior of Defendants, as alleged herein;

H. Order that Defendants restore and disgorge all funds to each employee acquired by means of any act or practice declared by this Court to be unlawful, unfair or fraudulent and, therefore, constituting unfair competition under Business and Professions Code §§ 17200, et seq.;

I. Grant incentive awards to Plaintiffs, as deemed reasonable by the Court;

J. Order Defendants to pay to Plaintiffs and Class Members all fines and penalties that apply under federal or state law;

K. Award Plaintiffs their reasonable attorneys' fees;

L. Award Plaintiffs the costs and expenses of this action; and

M. Grant to Plaintiffs all other and further relief as the Court deems to be equitable and just.

DEMAND FOR JURY TRIAL

PLAINTIFFS DEMAND A TRIAL BY JURY ON ALL TRIABLE ISSUES.

Respectfully submitted, this 6th day of January, 2017.

/s/ Adam M. Harrison

Adam M. Harrison (Admitted Pro Hac Vice)
aharrison@sawayalaw.com
David H. Miller (Admitted Pro Hac Vice)

dmiller@sawayalaw.com
THE SAWAYA & MILLER LAW FIRM
1600 Ogden Street
Denver, Colorado 80218
Phone: (303) 839-1650 x 1090
Fax: (303) 832-7102
Attorneys for Plaintiffs Price, Wilson and Esposito, on behalf of themselves and all others similarly situated

Plaintiffs' addresses:

Debra Price
c/o
David H. Miller
1600 Ogden Street
Denver, CO 80218

Sandra Jean Esposito
c/o
David H. Miller
1600 Ogden Street
Denver, CO 80218

Sean Wilson
c/o
David H. Miller
1600 Ogden Street
Denver, CO 80218

CERTIFICATE OF SERVICE

I hereby certify that on the 6th day of January, 2017, I electronically transmitted the attached document to the Clerk's Office using the CM/ECF system for filing, which transmitted a copy of this document to the following CM/ECF registrants:

Paul G. Karlsgodt
Casie Collignon
BAKER & HOSTETLER, LLP
1801 California Street, Suite 4400
Denver, CO 80202

Daniel B. Pasternak
SQUIRE PATTON BOGGS (US) LLP
One East Washington Street, Suite 2700
Phoenix, AZ 85004

/s/ Adam M. Harrison
Adam M. Harrison