IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

ELLEANOR SPANN, on behalf of herself and all others similarly situated,	:	
Plaintiff,	:	**Case No.** 20-cv-1005
v.	:	CLASS ACTION COMPLAINT
PAPERLESSPAY CORPORATION and **PRISMA HEALTH**,	:	DEMAND FOR JURY TRIAL
Defendants.	:	

Plaintiff **ELLEANOR SPANN**, on behalf of herself and all others similarly situated, brings this action against Defendants **PAPERLESSPAY CORPORATION** ("PaperlessPay") and **PRISMA HEALTH-MIDLANDS** ("PHM") (collectively "Defendants") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from the Defendants. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach involving Defendant PaperlessPay (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") of the Plaintiff, who was an employee of Defendant PHM, and the putative Class Members, all of whom are employees of Defendant PHM or of other entities whose payroll data is hosted on PaperlessPay's servers, including, without limitation, Marshall Medical Center ("MMC"), Community Memorial Health System ("CMHS"), Orlando Utilities

Commission ("OUC"), MP Environmental Services, Inc. ("MPE"), Fareway Stores, Inc. ("Fareway Stores") and Lee Auto Malls ("Lee Auto Malls").

2. The PII compromised in the Data Breach included highly sensitive information including first and last names, addresses, full bank account numbers, payroll and withholding information, and Social Security numbers of persons who were employed by Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores or Lee Auto Malls, among other entities serviced by PaperlessPay.

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

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

5. In addition, Defendant PaperlessPay (acting in the course and scope of its agency relationship with Defendant PHM) and its employees failed to properly monitor the computer network and systems that housed the PII. Had PaperlessPay properly monitored its property, it would have discovered the intrusion sooner.

6. Defendants maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant PaperlessPay's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendants and

thus Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

7. Defendants disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Member PII; and failing to take standard and reasonably available steps to prevent the Data Breach.

8. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the PII that Defendants collected and maintained is now in the hands of data thieves.

9. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

11. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

12. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

14. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of express contract, (iii) breach of implied contract; (iv) intrusion upon seclusion/invasion of privacy; and (v) breach of confidence.

II. JURISDICTION AND VENUE

15. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). There are at least 100 members in the proposed class, the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000.00 exclusive of interest and costs, and members of the Proposed Class, including Plaintiff, are citizens of states different from Defendant PaperlessPay.

16. Defendant PaperlessPay is a Florida corporation with its principal place of business in Jacksonville, Florida. PaperlessPay has sufficient minimum contacts in Florida, as it is a domestic corporation organized under the laws of the State of North Carolina and has its principal place of business in Florida, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

17. Defendant PHM is a South Carolina corporation with its principal place of business in Columbia, South Carolina.

18. This Court has jurisdiction over Defendant PHM through its business operations in this District, Defendant PHM intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper. Defendant PHM has sufficient minimum contacts in Florida as it does business in the State of Florida (through, among other things, its agent PaperlessPay) and the business being done in Florida directly relates to the subject of this lawsuit, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District.

III. PARTIES

20. Plaintiff Spann ("Spann") is and at all times mentioned herein was as individual citizen of South Carolina, residing in the city of Columbia. Plaintiff Spann is a former employee of PHM, having worked for PHM Palmetto Richland Emergency Room as a Cardia Care Monitor Technician from July 31, 2018, through June 20, 2020. She received notice of the Data Breach from PHM on or about July 20, 2020. A copy of the notice she received is attached hereto as Exhibit A (the "PHM Notice Letter").

21. Defendant PaperlessPay is a Florida corporation with its principal place of business at 800 Water Street, Jacksonville, FL 32204.

22. Defendant PHM is a South Carolina corporation with its principal place of business in Columbia, South Carolina.

IV. STATEMENT OF FACTS

A. Nature of Defendants' Businesses

23. Defendant PHM is in the business of providing healthcare services, medical care, and treatment to more than 1.2 million patients annually.

24. Defendant PHM offers a full spectrum of healthcare services and has on staff more than 32,000 employees.

25. Defendant PaperlessPay is a for-profit company specializing in processing payroll.

26. Defendant PHM uses PaperlessPay to produce electronic paystubs and W-2 forms for employees.

27. MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls also use PaperlessPay to produce electronic paystubs and W-2 forms for employees.

28. In the ordinary course of her employment at Defendant PHM, and as a condition of her employment, Plaintiff provided PII to Defendant PHM, including her name, address, full bank account number, and Social Security number.

29. In the ordinary course of their employment at MMC, CMHS, OUC, MPE, Fareway Stores or Lee Auto Malls, Class members, who are former or current employees of MMC, CMHS, OUC, MPE, Fareway Stores or Lee Auto Malls, provided PII to MMC, CMHS, OUC, MPE, Fareway Stores or Lee Auto Malls, including their name, address, full bank account number, and Social Security number.

30. Defendant PHM and Defendant PaperlessPay (in the course of providing its services and acting as an agent of PHM) maintain this PII on their servers and within their data infrastructure.

31. MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls and Defendant PaperlessPay (in the course of providing its services and acting as an agent of MMC, CMHS, OUC, MPE, Fareway Stores, and Lee Auto Malls) also maintain this PII on their servers and within their data infrastructure.

32. Upon information and belief, PHM has established a Privacy Policy wherein it details the PII it collects from employees and its standards to maintain the security and integrity of such data.[1]

33. The aim of the Privacy Policy is to provide adequate and consistent safeguards for the handling of employment data by PHM.

34. Defendant PHM, and by extension Defendant PaperlessPay, agreed to and undertook legal duties to maintain the PII entrusted to them by Plaintiff and Class Members safely, confidentially, and in compliance with all applicable laws.

35. Defendant PaperlessPay, acting as an agent of Defendant PHM, held the employee information collected by Defendant PHM at its servers located in Jacksonville, Florida.[2]

36. Defendant PaperlessPay, acting as an agent of MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls held the employee information collected by MMC, CMHS, OUC, MPE, PHM and Lee Auto Malls at its servers located in Jacksonville, Florida.

37. The employee information held by Defendant PaperlessPay in its computer systems and networks included the PII of Plaintiff and Class Members.

B. The Data Breach

38. On or about February 19, 2020, the Department of Homeland Security ("DHS") notified PaperlessPay that a dark web advertisement offered for sale "access" to PaperlessPay's SQL database server. The server contained Social Security numbers for current and former

---

[1] https://www.magellanhealth.com/privacy-policy/#:~:text=Magellan Health%20uses%20physical%2C%20technical%2C%20and,for%20providing%20service%20to%20you. (last visited June 25, 2020).

[2] *See* Notice Letter.

employees of PHM as well as that of current and former employees of other companies serviced by PaperlessPay.

39. Over the following weeks, PaperlessPay cooperated with the joint investigation conducted by ("DHS") and the federal Bureau of Investigation ("FBI").

40. PaperlessPay engaged the cybersecurity firm Ankura to investigate the incident. Ankura confirmed that, at a minimum, on February 18, 2020, an unauthorized individual entered the server which stored employee data for Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls and possibly staged an exfiltration from the server.

41. The data and files exfiltrated from Defendant PaperlessPay's computer servers included the PII of Plaintiff and Class Members, including first and last names, addresses, payroll and withholding information, full bank account numbers, and Social Security numbers.

42. On or about March 20, 2020, PaperlessPay notified Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls of the Data Breach.

43. PaperlessPay advised PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls that an unauthorized individual gained access to its server that hosts PHM' payroll data. PaperlessPay was unable to confirm the extent of the access, but it did confirm that an unauthorized individual gained access to it server at least once on February 18, 2020, and that the unauthorized individual had the ability to query any payroll data within the server.

44. As a result of PaperlessPay's disclosures, PHM decided to provide notice with an offer of one (1) year of credit monitoring and identify theft insurance without cost to its current and former employees, including Plaintiff Spann.[3]

45. As a result of PaperlessPay's disclosures, Fareway Stores decided to provide notice with an offer of one (1) year of credit monitoring without cost to 30,519 current and former employees.[4]

46. As a result of PaperlessPay's disclosures, OUC sent notice of the Data Breach to 2,100 potentially impacted current and former employees.[5]

47. As a result of PaperlessPay's disclosures, MMC sent notice of the Data Breach with an offer of one (1) year of identity monitoring without cost to its current and former employees.[6]

48. As a result of PaperlessPay's disclosures, CMHS sent notice with an offer of one (1) year of identity monitoring without cost to its current and former employees.[7]

49. As a result of PaperlessPay's disclosures, MPE decided to provide notice with an offer of two (2) years identity monitoring without cost to its current and former employees.[8]

---

[3] Notice of Data Breach, available at https://ago.vermont.gov/blog/2020/07/20/prisma-health-paperless-pay-notice-of-data-breach-to-consumers/; *see also* Exhibit A.

[4] Notice of Data Breach, available at https://www.iowaattorneygeneral.gov/media/cms/4162020_Fareway_Stores_Inc_961EEB88C3A3B.pdf.

[5] *See* https://www.orlandosentinel.com/news/crime/os-ne-ouc-data-breach-20200429-zhayied765asxcqesgqgbha664-story.html.

[6] Notice of Data Breach, available at https://oag.ca.gov/system/files/Breach%20notification%20letter%20-%20April%202020%20-%20template%20for%20AG.pdf.

[7] Notice of Data Breach, available at https://oag.ca.gov/system/files/%28CMHS%29%20Sample%20Notification%20Letter.pdf.

[8] Notice of Data Breach, available at https://media.dojmt.gov/wp-content/uploads/Breach-NotificationDetails-153.pdf.

50. As a result of PaperlessPay's disclosures, Lee Auto Malls decided to provide notice with an offer of two (2) years of identity monitoring without cost to its current and former employees.[9]

C. PHM Privacy Policy

51. Defendant PHM had an obligation created by contract, industry standards, common law, and representations made to Class Members, to keep Plaintiff and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

52. Plaintiff and PHM Subclass Members provided their PII to Defendant PHM with the reasonable expectation and mutual understanding that Defendant PHM would comply with its obligations to keep such information confidential and secure from unauthorized access.

53. Defendants data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the last few years.

54. Indeed, cyberattacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

55. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public.

56. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their

[9] Notice of Data Breach, available at https://ago.vermont.gov/blog/2020/04/15/lee-auto-malls-notice-of-data-breach-to-consumers/.

computer systems and data infrastructure. Defendants' unlawful conduct includes, but is not limited to, their failure to:

a. maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. adequately protect employees' PII;

c. properly monitor its own data security systems for existing intrusions;

d. ensure that vendors with access to payroll data employed reasonable security procedures;

57. As the result of computer systems in need of security upgrading, failure to implement proper cybersecurity hardware and software (such as next generation firewalls and multi-factor authentication), inadequate procedures for handling phishing emails, and inadequately trained employees, Defendants negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

58. Accordingly, Plaintiff and Class Members now face an increased risk of fraud and identity theft.

D. Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identify Theft

59. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which they noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[10]

[10] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited July 12) ("GAO Report").

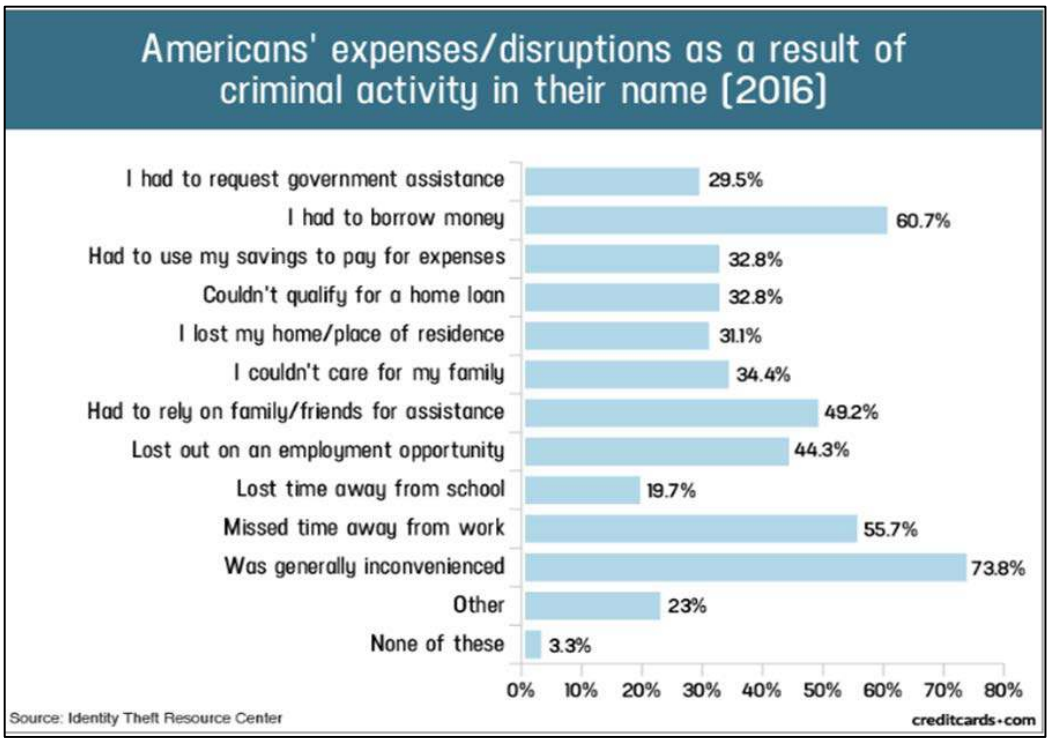
60. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[11]

61. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

62. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[12]

---

[11] *See* https://www.identitytheft.gov/Steps (last visited July 12, 2020).
[12] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited July 12, 2020).



63. What's more, theft of PII is also gravely serious. PII is a valuable property right.[13] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

64. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when they is discovered, and also between when PII and/or financial information is stolen and when they is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

[13] *See, e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

65. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

66. As evidenced by the dark web advertisement selling access to PaperlessPay's payroll database on the black market, there is a market for Plaintiff's and Class Members PII, and the stolen PII has inherent value.

67. As evidenced by the dark web advertisement selling access to PaperlessPay's payroll database on the black market, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

V. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

68. To date, Defendants have done absolutely nothing to compensate Class Members for the damages they sustained in the Data Breach other than offer to PHM Subclass Members identity monitoring services for 12 months through Experian.[14]

69. Defendant PHM's offer is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and they entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

---

[14] *See* Notice Letter.

70. Furthermore, Defendant PHM's credit monitoring offer squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendants merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.[15]

71. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their PII in the Data Breach.

72. Plaintiff's PII was compromised and exfiltrated by cyber criminals as a direct and proximate result of the Data Breach.

73. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

74. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

75. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

76. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

---

[15] *See* Notice Letter.

77. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

78. Plaintiff and Class Members also suffered a loss of value of their PII when they was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

79. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

80. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. finding fraudulent charges;

b. canceling and reissuing credit and debit cards;

c. purchasing credit monitoring and identity theft prevention;

d. addressing their inability to withdraw funds linked to compromised accounts;

e. taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. lacing “freezes” and “alerts” with credit reporting agencies;

g. spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. contacting financial institutions and closing or modifying financial accounts;

i. resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

81. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of the Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

82. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

83. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

84. Defendants' delay in identifying and reporting the Data Breach caused additional harm. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a

victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[16]

85. Indeed, once a Data Breach has occurred, "[o]ne thing that does matter is hearing about a Data Breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cyber criminals and warn other businesses of emerging dangers. If consumers don't know about a breach because they wasn't reported, they can't take action to protect themselves" (internal citations omitted).[17]

VI. CLASS ACTION ALLEGATIONS

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

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

> All persons whose PII was compromised in the Data Breach and who were sent Notice of the Data Breach (the "Class").

---

[16] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

[17] Consumer Reports, The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/

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

> All current and former employees of PHM whose PII was compromised in the Data Breach and who were sent Notice of the Data Breach (the "PHM Subclass").

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

90. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), 23(b)(2), 23(b)(3), and 23(c)(4).

91. Numerosity. The Members of the Class and Subclass are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of approximately no less than 64,619 current and former employees of Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Malls and the Subclass consists of approximately 32,000 current and former employees of Defendant PHM whose data was compromised in the Data Breach.

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

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

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

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

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

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

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

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

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

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

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

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

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

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

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

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

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

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

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

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

b. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

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

d. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

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

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

CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiff and all Class Members against Defendant PaperlessPay)

100. Plaintiff re-alleges and incorporates by reference all Paragraphs above as if fully set forth herein.

101. Plaintiff and Class Members were required to submit PII in order to obtain employment or as a condition of their employment.

102. By collecting and storing this data in PaperlessPay's computer property, PaperlessPay had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant PaperlessPay's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

103. Defendant PaperlessPay owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII.

104. Defendant PaperlessPay's had duty of care to use reasonable security measures because it was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

105. Defendant PaperlessPay's duty to use reasonable care in protecting confidential data also arose also because it is bound by industry standards to protect confidential PII.

106. Defendant PaperlessPay breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant PaperlessPay include, but are not limited to, the following:

107. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

a. Failing to adequately monitor the security of their networks and systems;

b. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised; and

e. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

108. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

109. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

110. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

111. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Breach of Express Contract
(On Behalf of Plaintiff and All Class Members against Defendant PaperlessPay)

112. Plaintiff re-alleges and incorporates by reference all Paragraphs above as if fully set forth herein.

113. Plaintiff and Class Members allege that they were the express, foreseeable, and intended third party beneficiaries, of valid and enforceable express contracts between Defendant PaperlessPay and Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores or Lee Auto Malls, contract(s) which (upon information and belief) include obligations to keep sensitive PII private and secure.

114. Defendant PaperlessPay materially breached its contractual obligation to protect the PII of Plaintiff and Class members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

115. The Data Breach was a reasonably foreseeable consequence of Defendant PaperlessPay's actions in breach of these contracts.

116. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII, the loss of control of their PII, the imminent risk of suffering additional damages in the future, and out-of-pocket expenses.

117. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

THIRD COUNT
Breach of Contract
(On Behalf of Plaintiff Spann and PHM Subclass Members against Defendant PHM)

118. Plaintiff re-alleges and incorporates by reference all Paragraphs above as if fully set forth herein.

119. Plaintiff and Class Members allege that PHM's privacy policy forms a binding contract between Fareway and its employees when they gave their PII to Fareway at the start of their employment.

120. Fareway breached these provisions of the contracts in that they did not have any measures to stop accidental loss or alteration or unauthorized access to protect Plaintiff and Class members' Personal Information, and did not limit access to that information to the specified individuals or entities. PHM violated its commitment to maintain the confidentiality and security of the PII of Plaintiffs and the class members and failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security.

121. The data breach reported on April 20, 2020 is a direct and legal cause of the injuries and damages suffered by Plaintiffs and the Class members.

122. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII, the loss of control of their PII, the imminent risk of suffering additional damages in the future, and out-of-pocket expenses.

123. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

FOURTH COUNT
Breach of Implied Contract
(On Behalf of Plaintiff Spann and PHM Subclass Members against Defendant PHM)

124. Plaintiff re-alleges and incorporates by reference all Paragraphs above as if fully set forth herein.

125. To the extent PHM privacy policy did not form an express contract, the creation of the employment relationship created implied contracts between PHM and the members of the PHM Subclass.

126. Fareway breached such implied warranties by failing to adhere to the terms of its privacy policy, violated its commitment to maintain the confidentiality of the PII of the members of the PHM Subclass and failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security.

127. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their PII, the loss of control of their PII, the imminent risk of suffering additional damages in the future, and out-of-pocket expenses.

128. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

FIFTH COUNT
Intrusion Upon Seclusion / Invasion of Privacy
(On behalf of Plaintiff and All Class Members against Defendant PaperlessPay and on behalf of Plaintiff and all PHM Subclass Members against Defendant PHM)

129. Plaintiff repeats and re-alleges each and every allegation contained in all Paragraphs above as if fully set forth herein.

130. The Restatement (Second) of Torts states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or her private affairs or concerns, is subject to liability to the other for invasion of her privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977)

131. Plaintiff and Class Members had a reasonable expectation of privacy in the PII Defendants mishandled. In failing to protect Plaintiff's and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

SIXTH COUNT
Breach of Confidence
(On behalf of Plaintiff and All Class Members against Defendant PaperlessPay and on behalf of Plaintiff and all PHM Subclass Members against Defendant PHM)

132. Plaintiff re-alleges and incorporates by reference all Paragraphs above as if fully set forth herein.

133. At all times during Plaintiff's and Subclass Members' interactions with Defendant PHM, Defendant PHM was fully aware of the confidential and sensitive nature of

Plaintiff's and Subclass Members' PII that Plaintiff and Class Members provided to Defendant PHM.

134. As the agent of Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall for purposes of storing, maintaining, and safeguarding Plaintiff's and Class Members' PII, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall duty to maintain confidence is imputed to Defendant PaperlessPay.

135. As alleged herein and above, Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall's relationship with Plaintiff and Class Members was governed by terms and expectations that Plaintiff and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed the unauthorized third parties.

136. Plaintiff and Class Members provided their respective PII to Defendant FAREWAY STORES, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall with the explicit and implicit understandings that Defendants would protect and not permit the PII to be disseminated to any unauthorized parties.

137. Plaintiff and Class Members also provided their PII to Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall with the explicit and implicit understandings that Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting their networks and data systems, including employees' email accounts.

138. Defendant PHM, MMC, CMHS, OUC, MPE, Fareway Stores and Lee Auto Mall voluntarily received in confidence Plaintiff's and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

139. Due to Defendants' failure to prevent, detect, avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiff's and Class Members' PII, Plaintiff's and Class Members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

140. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages.

141. But for Defendants' disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII, as well as the resulting damages.

142. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiff's and Class Members' PII. Defendants knew their computer systems and technologies for accepting and securing Plaintiff's and Class Members' PII had numerous security vulnerabilities.

143. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect,

contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

144. As a direct and proximate result of Defendants' breaches of its duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff pray for judgment as follows:

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

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

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

d. Ordering Defendants to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;

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

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

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

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

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

JURY TRIAL DEMANDED

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

Dated: September 4, 2020

Respectfully submitted,

/s/ *James Felman*
James Felman (FBN 775568)
Katherine Yanes (FBN 0159727)
Kynes Markman & Felman
PO Box 3396
Tampa, FL 33601-3396
Tel.: (813) 229-1118
Email: jfelman@kmf-law.com
kyanes@kmf-law.com

Gary E. Mason*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Email: gmason@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff