☐ YES ☑ NO

EXHIBITS

CASE NO. 2021 CH 6274

DATE: 12/17/2021

CASE TYPE: Class Action

PAGE COUNT: 44

CASE NOTE

_____

_____

_____

12-Person Jury

IN THE CIRCUIT COURT
FIRST JUDICIAL CIRCUIT
COOK COUNTY, ILLINOIS

GREGG NELSON, as an individual and on behalf of all others similarly situated,

Plaintiff,

vs.

BANSLEY & KIENER, L.L.P.,

Defendant.

CASE NO.: 2021CH06274

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Gregg Nelson ("Plaintiff") brings this Class Action Complaint against Bansley & Kiener, L.L.P. ("Bansley" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Bansley, an accounting firm that offers payroll and benefit compliance services to businesses, to seek damages for himself and other similarly situated payroll and/or benefit plan participants or any other person(s) impacted in the data breach at issue ("Participants" or "Class Members") who he seeks to represent, as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members. This action arises from Bansley's failure to properly secure and safeguard personal identifiable information, including without limitation, unencrypted and unredacted names, dates of birth, Social Security numbers, driver's license or state-issued identification numbers, passport numbers, tax identification numbers, military identification numbers, financial account numbers, payment card numbers, and/or personal health information (collectively, "personal identifiable information" or "PII").

2. Plaintiff alleges Bansley failed to provide timely, accurate and adequate notice to Plaintiff and Class Members whose employers or other business entities retained Bansley to manage their payroll, pension, health insurance, personal health information, and/or other benefits ("Bansley Clients" or "Clients"). Participants' knowledge about what personal identifiable information Bansley lost, as well as precisely what types of information was unencrypted and in the possession of unknown third parties, was unreasonably delayed by Bansley's unreasonable notification delay of approximately a year after it first learned of the data breach.

3. On or about December 3, 2021, Bansley notified state Attorneys General and many Participants about a widespread data breach involving sensitive PII of 274,115 individuals.[1] Bansley explained in its required notice letter that it discovered *on December 10, 2020* (almost exactly a year earlier) that its network had fallen victim to an "unauthorized person." This "data security incident resulted in the encryption" of certain of its network systems (the "Data Breach"). "Encryption of systems" is typically a defining characteristic of a ransomware attack.

4. In December 2020, Bansley chose not to notify affected Participants or, upon information and belief, its Clients, of its data breach instead choosing to address the incident in-house by making upgrades to some aspects of its computer security. It then simply resumed its normal business operations. Notice Letter, Ex. A.

5. Over five months later, on May 24, 2021, Bansley learned that Class Members' PII had been "exfiltrated" from its network. Only then did Bansley finally retain a cyber security firm to investigate this Data Breach. Notice Letter, Ex. A.

6. By August 24, 2021, the cyber security firm's professional investigation of Bansley's systems determined that Plaintiff's and Class Members' personal identifiable information (including but not limited to full names and Social Security numbers) was present and potentially stolen by the unauthorized person at the time of the incident. Notice Letter, Ex. A.

[1] Plaintiff's Notice Letter (attached as Exh. A) is dated November 24, 2021, which suggests that some notices were prepared and mailed slightly earlier.

7. However, according to information provided to the state Attorneys General, Bansley did not begin mailing notification letters to Class Members until December 3, 2021, almost exactly a year after the Data Breach was first discovered.[2]

8. Plaintiff in this action was, upon information and belief, a Participant in a payroll or benefits plan managed by Bansley for his employer. Prior to receiving the Data Breach Notice letter, Plaintiff was unaware that Bansley was performing payroll or benefits services on his behalf for his employer or any other business entity. The first that he learned of the Data Breach was on December 8, 2021 when he received by First Class U.S. Mail a Notice of Data Breach letter dated November 24, 2021 directly from Bansley. *See* **Exhibit A** ("Notice Letter").

9. In its Notice Letters, sent to Plaintiff, Class Members, and state and federal agencies, Bansley failed to explain why it took the company over six months (from May 24, 2021, when Bansley states its investigation determined that PII was accessed or acquired) to alert Class Members that their sensitive PII had been exposed.[3] As a result of this delayed response, Plaintiff and Class Members were unaware that their PII had been compromised, and that they were, and continue to be, at significant risk to identity theft and various other forms of personal, social, and financial harm.

10. Further, Bansley's Notice Letter to Plaintiff and Class Members does not explain that the Data Breach occurred between ***August 20, 2020 and December 1, 2020***—over a year before the Notice Letters were mailed.[4]

11. Plaintiff's and Class Members' unencrypted, unredacted PII was compromised due to Bansley's negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' sensitive data. Hackers obtained their PII because of its value in exploiting and

[2] Office of the Maine Attorney General, *Data Breach Notifications*, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741.shtml (last accessed December 10, 2021).
[3] *Id.*; *compare* Plaintiff's Notice Letter, Exh. A.
[4] *Id.*

stealing the identities of Plaintiff and similarly situated Class Members. The risks to these persons will remain for their respective lifetimes.

12. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Bansley's failure to: (i) adequately protect consumers' PII; (ii) warn consumers of its inadequate information security practices; and (iii) effectively monitor Bansley's network for security vulnerabilities and incidents. Bansley's conduct amounts to negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Bansley's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach, (v) charges and fees associated with fraudulent charges on their accounts, and (vi) the continued and certainly an increased risk to their PII, which remains in Bansley's possession and is subject to further unauthorized disclosures so long as Bansley fails to undertake appropriate and adequate measures to protect the PII. These risks will remain for the lifetimes of Plaintiff and Class Members.

14. Bansley disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or at the very least negligently failing to take and implement adequate and reasonable measures to ensure that its customers' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest

in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

15. Plaintiff Gregg Nelson is a resident and citizen of Wisconsin, residing in Hudson, St. Croix County, Wisconsin. Mr. Nelson received Bansley's *Notice of Data Breach*, dated November 24, 2021, on December 8, 2021, by First Class U.S. Mail. Exh. A.

16. Defendant Bansley & Kiener, L.L.P., is an Illinois limited liability partnership of certified public accountants, which has its principal place of business at 8745 West Higgins Road, Suite 200, Chicago, IL 60631.

17. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

18. All of Plaintiff's claims stated herein are asserted against Bansley and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this matter pursuant to Ill. Const. 1970, art. VI, § 9.

20. This Court has personal jurisdiction over Defendant for at least the following reasons: (i) Defendant regularly does business or solicits business, engages in other persistent courses of conduct and/or derives substantial revenue from products and/or services provided to individuals in Cook County and in the State of Illinois and (ii) Defendant has purposefully established substantial, systematic and continuous contacts with Cook County and the State of Illinois and expects or should reasonably expect to be in court here.

21. In short, Defendant has (more than) sufficient minimum contacts with this County such that this Court's exercise of jurisdiction over Defendant will not offend traditional notions of fair play and substantial justice.

22. Venue is proper in Cook County pursuant to 735 ILCS 5/2-101 because Defendant conducts its usual and customary business in this County and because a substantial portion of the events complained of occurred in this County.

IV. FACTUAL ALLEGATIONS

Background

23. Bansley and Kiener, L.L.P. is "a full-service CPA and advisory firm that delivers accounting, tax, consulting, and assurance solutions." It "supports privately held businesses, family-owned businesses, employee benefit plans, labor organizations, not-for-profits and individuals."[5]

24. In its Notice of Data Breach letter (Exh. A), Bansley claims that "information and security are among our highest priorities" and further asserts that it has "strict security measures in place to protect information in our care."

25. On its own website, Bansley holds itself out as a member of the American Institute of Certified Public Accountants (AICPA), which Bansley explains sets ethical standards for the accounting profession, offers specialty credentials, provides it with the training, skills, services, and information necessary for Bansley to stay at the top of its profession.[6] As a member of this organization, Bansley has instant access to the wealth of knowledge AICPA offers regarding protection of customers' PII.[7]

---

[5] *See* Bansley and Kiener, L.L.P. website, http://www.bk-cpa.com/ (last accessed December 10, 2021).

[6] *See* http://www.bk-cpa.com/other-bk-member-affiliation-resources/ (last accessed December 10, 2021).

[7] *See e.g.,* https://www.aicpa.org/search/privacy, first article: *Cyberattacks, Data Breaches, and Privacy: Walk through the causes of data breaches and implications, and the appropriate responses.* (last accessed December 10, 2021).

26. In addition, Bansley states that it is a member of the Illinois CPA Society (ICPAS),[8] which also provides it with immediate access to continuing education, articles, seminars, and other knowledge resources that stress the critical need of protecting customers' PII.[9]

27. As Bansley acknowledges in its Notice Letters, protection of personal identifiable information is one of the "highest priorities" for businesses managing payroll and benefits data.

28. Plaintiffs and the Class Members, as persons for whom Bansley currently or in the recent past managed their payroll and or benefits plans, reasonably relied (directly or indirectly) on this sophisticated accounting entity to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Employees and benefit plan participants, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

29. Bansley had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

30. In late November 2021, Bansley first began notifying Class Members and state Attorneys General ("AGs") about a widespread data breach of its computer systems and involving the sensitive personal identifiable information of persons.[10] Bansley explained—but upon information and belief, only to the AGs—that the Data Breach occurred from August 20, 2020, through December 1, 2020.[11]

31. According to its Notice Letters, on December 10, 2020 Bansley "identified a data security incident that resulted in the encryption of certain systems within [its] environment."[12]

---

[8] *See* http://www.bk-cpa.com/other-bk-member-affiliation-resources/ (last accessed December 10, 2021).
[9] *See, e.g.*, https://www.icpas.org/information/technology-resources/disruptive-technologies (last accessed December 10, 2021).
[10] Office of the Maine Attorney General, *Data Breach Notifications*, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741.shtml (last accessed December 10, 2021).
[11] *Id.*
[12] *Id.*

Bansley claimed that it "addressed the incident, made upgrades to certain aspects of [its] computer security, restored the impacted systems from recent backups, and resumed normal operation." The firm claims it "believed at the time that the incident was fully contained and did not find any evidence that information had been exfiltrated from [its] environment."[13]

32. However, Bansley acknowledged that on May 24, 2021, it learned personal identifiable information had been exfiltrated by an unauthorized person. Bansley only launched an investigation and retained an outside cyber security firm to investigate this Data Breach after this date.[14]

33. By August 24, 2021, Bansley knew that an unauthorized individual or individuals hacked into and had access to the PII in its systems between August 20, 2020 and December 1, 2020, in other words, the unauthorized access occurred for one hundred and three (103) calendar days.[15]

34. As its notice to the AGs acknowledges, Bansley's failure to protect its systems exposed **274,115 Class Members'** confidential Personal Identifiable Information, entrusted to Bansley's care as a major accounting firm, to criminals.[16]

35. The confidential information that was accessed without authorization included persons' full names along with their Social Security number.[17]

36. Upon information and belief, the PII was not encrypted prior to the data breach.

37. Upon information and belief, the cyberattack was targeted at Bansley as a payroll, benefits, and financial management accounting firm that collects and maintains valuable personal, tax, and financial data from its many Clients, as well as employees and benefit plan participants of those Clients.[18]

---

[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id*.
[17] *Id.*
[18] *See* http://www.bk-cpa.com/ (last accessed December 10, 2021).

38. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

39. Beginning on or about November 24, 2021, Bansley sent affected persons (including Plaintiff Nelson) a *Notice of Data Breach*, informing the recipients of the notice that their confidential data was involved, and stating:

> . . . Upon learning of the incident, and to help prevent something like this from happening in the future, we have taken steps to confirm and further strengthen the security of our systems, including deploying SentinelOne Endpoint Detection & Response software on the computers in our environment, upgrading our filtering capabilities to block traffic from malicious sources, establishing and reviewing permissions for secure file share portals, resetting user passwords, and transferring sensitive data to cloud storage. We also continue to educate our employees on cyber security best practices. . . .
>
> As a precautionary measure, we also secured the services of Kroll to provide identity monitoring services at no cost to you for one (1) year. Your identity monitoring services include credit monitoring, fraud consultation, and identity theft restoration. . . .
>
> Further, it is always advisable for you to regularly review your financial account statements and credit reports for unauthorized activity. If you notice such activity, you should immediately report it to the relevant financial institution or the credit bureau reporting the activity. You may also review the information contained in the enclosed "Additional Steps You Can Take."[19]

[19] https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741.shtml (last accessed December 10, 2021); *see also* Exh. A.

40. In its "ADDITIONAL STEPS YOU CAN TAKE" attachment, Bansley suggests efforts its victims can take, including among other suggestions spending time:

a. Activating identity monitoring services;

b. Reviewing account statements;

c. Reviewing free credit reports for any unauthorized activity;

d. Contacting the Federal Trade Commission and/or the Attorney General's office in the person's state;

e. Setting up fraud alerts and credit/security freezes; and

f. When necessary, filing a police report to report identity theft.

41. Bansley admitted in its *Notice of Data Breach* to the Attorneys General that their systems were subjected to unauthorized access between August 20, 2020,[20] and December 1, 2020, however those dates were not included on the notice letters sent to Plaintiff and Class Members.[21] Bansley made no indication to either group (AGs or Class) that the exfiltrated PII was retrieved from the cybercriminals who took it.

42. With its offer of credit and identity monitoring services, Bansley is acknowledging that the impacted persons are subject to an imminent threat of identity theft and financial fraud.

43. In response to the Data Breach, Bansley claims, "we have taken steps to confirm and further strengthen the security of our systems."[22] Bansley admits enhanced "upgrading our filtering capabilities" was required, but there is no indication whether these steps are adequate to protect Plaintiff's and Class Members' PII going forward.

44. Bansley had obligations created by contract, industry standards, common law, and representations made to its Clients to keep the PII of Plaintiff and Class Members that was entrusted to Bansley's Clients confidential. and to protect the PII from unauthorized access and disclosure.

---

[20] *Id.*
[21] *See* Exh. A.
[22] *Id*.

45. Plaintiff and Class Members provided their PII to Bansley, either directly or through Bansley's Clients (employers or other business entities) with the reasonable expectation that Bansley as an accounting firm would comply with its duty and obligations and representations to keep such information confidential and secure from unauthorized access.

46. Bansley failed to uphold its data security obligations to Plaintiff and Class Members. As a result, Plaintiff and Class Members are significantly harmed and will be at a high risk of identity theft and financial fraud for many years to come.

47. Bansley did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

Securing PII and Preventing Breaches

48. Bansley could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

49. In its notice letters, Bansley acknowledged the sensitive and confidential nature of the PII. To be sure, collection, maintaining, and protecting PII is vital to virtually all of Bansley's business purposes as certified public accountants. Bansley acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Ransomware Attack and Data Breach were Foreseeable Risks of which Defendant was on Notice

50. It is well known that PII, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

51. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[23]

[23] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed December 10, 2021)

52. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[24]

53. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[25]

54. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

55. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all problems … and won't guarantee … a fresh start."

56. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Bansley knew or should have known that its electronic records would be targeted by cybercriminals.

[24] *Id*.
[25] *Id* at p. 15.

57. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

58. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, Bansley failed to take appropriate steps to protect the PII of Plaintiffs and the proposed Class from being compromised.

At All Relevant Times Bansley Had a Duty to Plaintiff and Class Members to Properly Secure their Private Information

59. At all relevant times, Bansley had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Bansley became aware that their PII may have been compromised.

60. Bansley's duty to use reasonable security measures arose as a result of the special relationship that existed between Bansley, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class entrusted Bansley with their PII when they or their employers or other business entities entrusted Bansley to manage their payroll and benefits accounts.

61. Bansley had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Bansley breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

62. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

63. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[26] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[27]

64. The ramifications of Bansley's failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personal Identifiable Information

65. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200,

[26] 17 C.F.R. § 248.201 (2013).
[27] *Id*.

and bank details have a price range of $50 to $200.[28] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[29]

66. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[30]

67. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of

---

[28] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed December 10, 2021).

[29] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed December 10, 2021).

[30] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed December 10, 2021).

misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

68. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[31]

69. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[32]

70. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[33]

71. Given the nature of Bansley's Data Breach, as well as the length of the time Bansley's systems were breached and the long delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

72. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

---

[31] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed December 10, 2021).

[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed December 10, 2021).

[33] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

breach, because credit card victims can cancel or close credit and debit card accounts.[34] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

73. To date, Bansley has offered its consumers *only one year* of identity monitoring services, despite the long period of exposure (over 100 days) and the approximately yearlong delay from their discovery of the Data Breach to the Notice Letters. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

74. The injuries to Plaintiff and Class Members were directly and proximately caused by Bansley's failure to implement or maintain adequate data security measures for its current and former customers.

Bansley Failed to Comply with FTC Guidelines

75. Federal and State governments have established security standards and issued recommendations to lessen the risk of data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[35]

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[36] The guidelines note businesses should protect the personal consumer and

---

[34] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed December 10, 2021).

[35] Federal Trade Commission, *Start With Security, available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 10, 2021).

[36] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed December 10, 2021).

consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

77. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[37]

78. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

[37] FTC, *Start with Security*, *supra* note 34.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

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

80. Because Class Members entrusted Bansley with their PII directly or indirectly through Bansley's Clients, Bansley had, and has, a duty to the Class Members to keep their PII secure.

81. Plaintiff and the other Class Members reasonably expected that when they provide PII to their employers or entities through which they receive benefits, that the accounting firm hired for management of payroll or benefits—here, Bansley—would safeguard their PII.

82. Bansley was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiff and members of the Classes. Bansley was also aware of the significant repercussions if it failed to do so.

83. Bansley's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiff's and Class Members' full names, Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Have Suffered Concrete Injury As A Result Of Defendant's Inadequate Security And The Data Breach It Allowed.

84. Plaintiff and Class Members reasonably expected that Defendant would provide adequate security protections for their PII, and Class Members provided Defendant with sensitive personal information, including their Social Security numbers and driver's license numbers.

85. Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant for its service, whether directly or indirectly through their employers or business entities, Plaintiff and other reasonable consumers understood and expected that their PII would be protected with data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members, through Bansley's Clients, received services that were of a lesser value than what they reasonably expected. As such, Plaintiff and the Class Members suffered pecuniary injury.

86. Cybercriminals capture PII to exploit it; the Class Members are now, and for the rest of their lives will be, at a heightened risk of identity theft. Plaintiff has also incurred (and will

continue to incur) damages in the form of, *inter alia*, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

87. The cybercriminals who obtained the Class Members' PII may exploit the information they obtained by selling the data in so-called "dark markets." Having obtained these names, addresses, Social Security numbers, and other PII, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

88. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

89. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiff and the other Class Members have been deprived of the value of their PII, for which there is a well-established national and international market.

90. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.[38]

91. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the other Class Members at an imminent, immediate, and

[38] *Id.*

continuing increased risk of identity theft and identity fraud.[39] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[40] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[41] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

92. As a result of the Data Breach, Plaintiff and Class Members have already suffered damages.

93. In its Notice Letter, Defendant represented to the Class Members and AGs that it initially discovered the Data Breach on December 10, 2020, but "believed at the time that the incident was fully contained and did not find any evidence that information had been exfiltrated from our environment."[42] As EmiSoft, an award-winning malware-protection software company, states "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence, *especially during the preliminary stages of the investigation*."[43]

94. On May 24, 2021, Bansley admits that it was "made aware that certain information had been exfiltrated from our environment by an unauthorized person[,]" yet by the date of the

---

[39] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), http://www.iii.org/insuranceindustryblog/?p=267 (last accessed December 10, 2021).

[40] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed December 10, 2021).

[41] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, (*available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed December 10, 2021).

[42] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741.shtml (last accessed December 10, 2021); *see also* Exh. A.

[43] EmiSoft Malware Lab, *The chance of data being stolen in a ransomware attack is greater than one in ten* (EMISOFT BLOG July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/ (last accessed December 13, 2021, emphasis added)).

notice letters, it still claimed to be "unable to determine whether the unauthorized actor actually viewed any of the information." [44] It is likely that the cybercriminals did steal data and did so undetected.

95. In this case, according to Defendant's notification to the state Attorneys General, cybercriminals had access to Class Members' data from at least August 20, 2020, to December 1, 2020, yet its notice letters about that Data Breach did not go out until almost exactly a year later. This is tantamount to the cybercriminals have a year-long head start on stealing the identities of Plaintiff and Class Members.

96. Accordingly, that Defendant has not found evidence of data being viewed is not an assurance that the data were not accessed, acquired, and stolen. Indeed, the likelihood that cybercriminals stole the data covertly is significant, likely, and concerning.

Plaintiff Nelson's Experience

97. On or about December 8, 2021, Mr. Gregg Nelson, a citizen and resident of Hudson, Wisconsin, received Notice of Data Breach Letter dated November 24, 2021 by US. Mail.

98. At the time that he received the Notice Letter, he was unaware of why his Personal Identifying Information had been entrusted in Bansley's care. Based on the language in the letter, he assumed at the time of receipt (and still assumes) that Bansley's is the accounting firm that his employer has retained to manage his and co-workers' payroll and/or benefits.

99. At the time of his employment, he provided his PII to his employer in order to get paid and receive employment benefits and because under state and federal law, he was required to do so. He reasonably relied on any certified public accounting firm retained by his employer to protect the security of his PII.

100. As a result of the Data Breach and the information that he received in the Notice Letter, Mr. Nelson spends approximately a half hour per day dealing with the consequences of the Data Breach (self-monitoring his bank and credit accounts), as well as his time spent verifying the

[44] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/36b0a9a6-30c4-4942-9095-aaf86cfba741.shtml (last accessed December 10, 2021); *see also* Exh. A.

legitimacy of the *Notice of Data Breach*, communicating with Bansley representatives, communicating with his bank, exploring credit monitoring and identity theft insurance options, signing up for the credit monitoring supplied by Bansley, and reporting the breach to the IRS and FTC. This time has been lost forever and cannot be recaptured.

101. Mr. Nelson is very careful about sharing his own personal identifying information and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

102. Mr. Nelson stores any and all documents containing PII in a secure location and destroys any documents he receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise his identity and credit card accounts. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

103. Mr. Nelson suffered actual injury and damages through his payroll and benefits accounts due to Bansley's mismanagement of his PII before the Data Breach.

104. Mr. Nelson suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Bansley for the purpose of providing him payroll and benefit services, which was compromised in and as a result of the Data Breach.

105. Mr. Nelson suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach, and he has suffered anxiety and increased concerns for the theft of his privacy since he received the Notice Letter. He is especially concerned about the theft of his full name paired with his Social Security number.

106. Mr. Nelson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third-parties and possibly criminals.

107. Mr. Nelson has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Bansley's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

108. Plaintiff brings this nationwide class action on behalf of himself and on behalf of all others similarly situated.

109. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> All persons residing in the United States whose PII was compromised in the data breach first announced by Bansley on or about December 3, 2021 (the "Nationwide Class").

110. The Wisconsin Subclass is defined as follows:

> All persons residing in Wisconsin whose PII was compromised in the data breach first announced by Bansley on or about December 3, 2021 (the "Wisconsin Subclass").

111. The above class and subclasses are herein referred to as the "Classes."

112. Excluded from the Classes are the following individuals and/or entities: Bansley & Kiener, L.L.P., and Bansley's parents, subsidiaries, affiliates, officers and directors, and any entity in which Bansley has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

113. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

114. **Numerosity – 735 ILCS 5/2-801(1)**: Classes are so numerous that joinder of all members is impracticable. Bansley has identified and sent notice to over 274,000 persons whose PII may have been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Bansley's records.

115. **Commonality and Predominance – 735 ILCS 5/2-801(2)**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Bansley had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Bansley had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Bansley had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Bansley failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Bansley actually learned of the Data Breach;

f. Whether Bansley adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Bansley violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

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

i. Whether Bansley adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Bansley breached express or implied contracts – contracts of which Plaintiff and Class Members were third-party beneficiaries -- by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual damages, nominal damages, and/or punitive damages as a result of Bansley's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of

Bansley's wrongful conduct, and;

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

116. Defendant engaged in a common course of conduct giving rise to the legal rights Plaintiff seeks to enforce, on behalf of herself and the other members of the Classes, 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 Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale in comparison, in both quality and quantity, to the numerous common questions that dominate this action. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

117. **Policies Generally Applicable to the Class**: This class action is also appropriate for certification because Bansley has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Bansley's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Bansley's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

118. **Adequacy of Representation – 735 ILCS 5/2-801(3):** Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to that of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

119. **Superiority – 735 ILCS 5/2-801(4)**: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Bansley. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

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

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

122. Adequate notice can be given to Class Members directly using information maintained in Bansley's records.

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

124. Further, Bansley has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, the Subclass)

125. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

126. As a condition of any person or entity using the payroll and benefit management services of Bansley, Participants are obligated to provide Bansley with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

127. Plaintiff and Class Members entrusted their PII to Bansley on the premise and with the understanding that Bansley would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

128. Bansley has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

129. Bansley knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of their consumers' PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

130. Bansley had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to

unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Bansley's security protocols to ensure that Plaintiff's and Class Members' information in Bansley's possession was adequately secured and protected.

131. Bansley also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

132. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Bansley's business as certified public accountants and its training and continuing education requirements in this field, for which the diligent protection of PII is a continuous forefront issue. *See, e.g.,* a multitude of resources related to "data breach" on American Institute of Certified Public Accountants (https://www.aicpa.org/search/data+breach, locating 826 hits on December 13, 2021), which is cited on Bansley's website (http://www.bk-cpa.com/other-bk-member-affiliation-resources/).

133. Plaintiff and Class Members were the foreseeable and probable victims of Bansley's inadequate security practices and procedures. Bansley knew of should have known of the inherent risks in collecting and storing the PII of Plaintiff and Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Bansley's systems.

134. Bansley's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Bansley's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Bansley's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Bansley.

135. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Bansley's possession.

136. Bansley was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

137. Bansley had and continues to have a duty to adequately and promptly disclose that the PII of Plaintiff and Class Members within Bansley's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

138. Bansley had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

139. Bansley has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

140. Bansley, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and Class Members during the time the PII was within Bansley's possession or control.

141. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

142. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

143. Bansley improperly and inadequately safeguarded the PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

144. Bansley failed to heed industry warnings and alerts to provide adequate safeguards to protect consumers' PII in the face of increased risk of theft.

145. Bansley, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its consumers' PII.

146. Bansley, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

147. But for Bansley's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and Class Members would not have been compromised.

148. There is a close causal connection between Bansley's failure to implement security measures to protect the PII of Plaintiff and Class Members and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Bansley's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

149. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Bansley, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Bansley's duty in this regard.

150. Bansley violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Bansley's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

151. Bansley's violation of Section 5 of the FTC Act constitutes negligence *per se*.

152. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

153. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses,

which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

154. As a direct and proximate result of Bansley's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Bansley's possession and is subject to further unauthorized disclosures so long as Bansley fails to undertake appropriate and adequate measures to protect the PII of consumers in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Bansley's goods and services they received.

155. As a direct and proximate result of Bansley's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

156. Additionally, as a direct and proximate result of Bansley's negligence and negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remains in Bansley's possession and is subject to further unauthorized disclosures so long as Bansley fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, on behalf of the Subclass)

157. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

158. Plaintiff and Class Members conferred a monetary benefit on Defendant in the form of monetary payments—directly or indirectly—for providing payroll and benefit compliance services for the Clients.

159. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits conferred by the Clients on behalf of the Plaintiff and Class Members.

160. The money that Clients paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

161. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

162. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

163. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and that the Clients paid for.

164. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff and Class Members' PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms

of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiff and the Nationwide Class
Or in the alternative, on behalf of the Subclass)

165. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

166. This count is pled in the alternative to Count II (Unjust Enrichment).

167. Plaintiff and Class Members allege that they were the express, foreseeable, and intended third-party beneficiaries of valid and enforceable express contracts between Defendant and its Clients (including the Clients who were the employers of Plaintiff and Class Members), contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

168. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all employees or former employees of Clients entering into the contracts), as Defendant's service was to aid the Clients in not only paying and conducting other beneficial payroll and benefits plan administration services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services.

169. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

170. The contract was therefore made primarily for the benefit of Plaintiff and Class Members, with Defendant promising to maintain the security of Plaintiff's and Class Members' PII while the Clients used Defendant's services to pay and otherwise benefit Plaintiff and Class Members.

171. Defendant 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.

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

173. 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 of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

174. Plaintiff and Class Members are entitled to compensator, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, on behalf of the Subclass)

175. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

176. This count is plead in the alternative to Count II (Unjust Enrichment).

177. Upon information and belief, Plaintiff's and Class Members' PII was provided to Defendant as part of the payroll and benefits plan administration services that Defendant provided to its Clients.

178. In exchange, Defendant's Clients (including the Employers and former Employers of Plaintiff and Class members) agreed to pay Defendant money for these payroll and benefits plan administration services.

179. Plaintiff and Class Members are the intended third-party beneficiaries to the contracts entered into between their Employers or former Employers (or other business entities) and Defendant.

180. By providing payroll and benefits plan administration services for the Clients (including the Employers and former Employers of Plaintiff and Class Members), Defendant and

the Clients entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

181. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

182. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

183. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

184. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

185. Defendant further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

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

187. As a result of Defendant's conduct, Plaintiff, Class Members, and the Clients did not receive the full benefit of their bargain.

188. Had Defendant disclosed that its data security was inadequate, neither the Clients, Plaintiff, Class Members, nor any reasonable person or business entity like the Clients would have entered into such contracts with Defendant.

189. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

190. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

191. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long-term credit monitoring to all Class Members.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class, or in the alternative, on behalf of the Subclass)

192. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

193. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. §2201.

194. Plaintiff and Class Members entered into an implied contract that required Defendant to provide adequate security for the PII it collected from Plaintiff and Class Members.

195. Defendant owes a duty of care to Plaintiff and Class Members requiring them to adequately secure PII.

196. Defendant still possesses PII regarding Plaintiff and Class Members.

197. Since the Data Breach, Defendant has announced few if any specific and significant changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and, thereby, prevent further attacks.

198. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and Class Members. In fact, now that Defendant's insufficient data security is known to hackers, the PII in Defendant's possession is even more vulnerable to cyberattack.

199. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

200. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

201. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with their contractual obligations and duties of care to provide adequate security, and (2) that to comply with their contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
d. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is

compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant not transmit PII via unencrypted email;

f. Ordering that Defendant not store PII in email accounts;

g. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

h. Ordering that Defendant conduct regular computer system scanning and security checks;

i. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

j. Ordering Defendant to meaningfully educate their current, former, and prospective customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class Members, requests judgment against Bansley and Kiener, L.L.P. and that the Court grant the following:

A. For an Order certifying the Nationwide Classes or, in the alternative, the Subclass as defined herein, and appointing Plaintiff and his Counsel to represent the certified Nationwide Class and Subclass;

B. For equitable relief enjoining Bansley from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class, including but not limited to an order:

i. prohibiting Bansley from engaging in the wrongful and unlawful acts described herein;

ii. requiring Bansley to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Bansley to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Bansley can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class;

iv. requiring Bansley to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Bansley from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Bansley to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Bansley's systems on a periodic basis, and ordering Bansley to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Bansley to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Bansley to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Bansley to segment data by, among other things, creating firewalls and access controls so that if one area of Bansley's network is compromised, hackers cannot gain access to other portions of Bansley's systems;

x. requiring Bansley to conduct regular database scanning and securing checks;

xi. requiring Bansley to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Bansley to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Bansley to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Bansley's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Bansley to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Bansley's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Bansley to meaningfully educate all class members about the threats that they face as a result of the loss of their confidential personal identifying

information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Bansley to implement logging and monitoring programs sufficient to track traffic to and from Bansley's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Bansley's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: December 17, 2021

Respectfully Submitted,

/s/ *Gary M. Klinger*

Gary M. Klinger
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (202) 429-2290
Fax: (202) 429-2294
gklinger@masonllp.com

Gary E. Mason
David K. Lietz
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294
dlietz@masonllp.com
gmason@masonllp.com

Attorneys for Plaintiff and the Proposed Classes

ClassAction.org
