UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

KEVIN PAYNE, individually and on behalf of all others similarly situated, Plaintiff, v. TRULIANT FEDERAL CREDIT UNION, and DOXIM, INC. Defendants.	Case No. **CLASS ACTION** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff Kevin Payne ("Plaintiff"), on behalf of himself and all others similarly situated (the "Class" or "Class Members"), files this Class Action Complaint ("Complaint") against Defendants Truliant Federal Credit Union ("Truliant"), and Doxim, Inc ("Doxim") (collectively, "Defendants") and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to safeguard and secure the personally identifiable information ("PII") of data breach victims, including Plaintiff (the "Class" or "Class Members").

2. The information affected was provided by Truliant's customers, including Plaintiff and Class Members, through a cybersecurity attack on Doxim, a third-party print and digital document and statement provider of Truliant (the "Data Breach").[1]

[1] Richard Craver, *Truliant Customer Information Leaked In Data Breach*, May 29, 2024, https://journalnow.com/news/local/truliant-discloses-data-breach-tied-to-former-third-party-vendor/article_1d5d0554-1d41-11ef-93e5-d3c820fcc4a5.html ("Truliant said in a letter dated May 14 that Doxim told the credit union of an April 22 cybersecurity attack that affected members.")

3. Truliant is a federally charted Triad-based credit union that provides financial services to its members. Truliant contracted with Doxim for print and digital document and statement services.

4. Although Truliant has ended the contract with Doxim "due to the production issues experienced earlier this year[]"[2], Doxim has collected and maintained this sensitive PII in its possession for the purpose of its print and digital document and statement services.

5. The data exposed in the breach includes some of the most sensitive types of data that cybercriminals seek in order to commit fraud and identity theft. As a result of Defendants' negligence, between April and May 2024, cybercriminals were able to gain access to Defendants' data records and access this sensitive and valuable PII (the "Data Breach"). On information and belief, information disclosed in the Data Breach includes but is not limited to names, Social Security numbers, account number and other financial information.

6. On its website, Truliant states that "Truliant Federal Credit Union will take all the steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information."[3]

7. Truliant contracts with "third party companies and individuals to facilitate our Service ("Service Providers"), provide the Service on [its] behalf, perform Service-related services or assist [it] in analyzing how [its] Service is used. These third parties have access to [customers']

[2] *See Id.*
[3] Truliant Privacy Policy, Transfer of Data, https://www.truliantfcu.org/security-center/privacy-policy (last visited June 12, 2024).

Personal Data only to perform these tasks on [its] behalf and are obligated not to disclose or use it for any other purpose."[4]

8. According to the notice letter from Truliant to its customers, dated May 14, 2024, "[o]n April 22, 2024, [its] former third-party print and digital document and statement provider, Doxim, notified [it] of a cybersecurity attack that resulted in unauthorized access to some of their data files including Truliant files from 2012. These compromised files contained a combination of some of all of the following categories of information for each affected member: member name, account number, and Social Security number. Some of [the customers'] information in these categories was included on the compromised files."

9. More than 48,000 Truliant customers had their Personal Information compromised in the Data Breach. Although not disclosed in the Notice Letter, based on information and belief, Class Members' addresses and dates of birth might have been impacted as well. [5]

10. As a result of Defendants' failure to protect the consumer information they were entrusted to safeguard, Plaintiffs and Class Members suffered a loss of the value of their Personal Information, and have been exposed to or are at imminent and significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future.

11. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial information in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, and using Class Members' PII to target other phishing and hacking intrusions.

---

[4] *Id*. Service Providers.

[5] Truliant Federal Credit Union Reports Third Party Data Breach, May 29, 2024, https://beyondmachines.net/event_details/truliant-federal-credit-union-reports-third-party-data-breach-w-d-5-8-x

12. Defendants owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Class Members' PII from unauthorized access and disclosure.

13. As a result of Defendants' inadequate security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class Members' PII was accessed and disclosed. This action seeks to remedy these failings and the harm caused to Plaintiff and Class Members as a result. Plaintiff brings this action on behalf of himself and all persons whose PII was exposed as a result of the Data Breach.

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

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

16. Plaintiff, on behalf of himself and all other Class Members, asserts claims for negligence, negligence *per se*, breach of fiduciary duty, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

17. Plaintiff Kevin Payne resides in Forsyth County, North Carolina. Mr. Payne received a letter from Truliant dated May 14, 2024 informing him of the Data Breach.

18. Plaintiff has been forced to spend time and money addressing and attempting to mitigate further harm and injury resulting from the Data Breach. In response to learning his PII was exposed in the Data Breach, Plaintiff spent time, money, and effort including but not limited to purchasing credit and identity thief protection services. Plaintiff has experienced an increase in spam calls and emails since the Data Breach. Plaintiff has also suffered emotionally over the stress resulting from the Data Breach and his substantially increased risk of identity theft, such as the possibility of criminals using his PII to open bank accounts or commit other fraud under his name. Plaintiff is working on building his credit. At this crucial time, any negative impact on his credit resulting from the Data Breach would seriously affect his financial plan.

19. Plaintiff was required to provide his PII, or to allow his PII to be provided, to Defendants as a condition of receiving financial services from Truliant. Doxim collects and stores PII to perform its services for Truliant. Plaintiff does not have any ability to protect his PII that was or remains in Defendants' possession.

20. Defendant Truliant is a federally chartered cooperative association with its principal place of business in Winston-Salem, North Carolina. In the regular course of its business, Defendant Truliant takes custody of and maintains control over PII from its customers.

21. Defendant Doxim is headquartered in Ontario, Canada, with approximately four (4) offices in the United States, in Indianapolis, Las Vegas, Madison Heights, and New York. Defendant Doxim regularly conducts business within the state of North Carolina, and takes

custody of and maintains control over PII from Truliant's customers, including Plaintiff and Class Members.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) because (a) there are 100 or more Class Members, (b) at least one Class Member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the aggregate matter in controversy exceeds $5,000,000, exclusive of interests and costs.

23. This Court has general personal jurisdiction over Defendant Truliant because Defendant Truliant is a citizen of North Carolina. Moreover, Defendant Truliant has sufficient minimum contacts in the State, and Defendant Truliant engaged in the conduct underlying this action in North Carolina, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class Members' PII. Defendant Truliant intentionally availed itself of this jurisdiction by marketing and selling services and accepting and processing payments for those services within the State.

24. This Court has general personal jurisdiction over Defendant Doxim because Defendant Doxim has sufficient minimum contacts in the State, and Defendant Truliant engaged in the conduct underlying this action in North Carolina, including the collection, storage, and inadequate safeguarding of Plaintiff's and Class Members' PII. Defendant Truliant intentionally availed itself of this jurisdiction by marketing and selling services and accepting and processing payments for those services within the State.

25. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant Truliant resides in this District, a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and both Defendants do business in this District.

FACTUAL ALLEGATIONS

Overview of Defendants

26. Defendant Truliant is a federally charted Triad-based credit union that provides financial services to its individuals and businesses, including "Bank", "Borrow", "Insure", and "Invest".[6] Truliant was chartered in 1952 to serve the employees of Western Electric and was known as Radio Shops Credit Union. Truliant currently serves over 300,000 members with more than 30 locations across the Carolinas and Virginia, and over $4 billion in assets.[7]

27. On its website, Truliant states that "Truliant Federal Credit Union will take all the steps reasonably necessary to ensure that your data is treated securely and in accordance with this Privacy Policy and no transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place including the security of your data and other personal information."[8]

28. Truliant contracts with third party companies and individuals, including Defendant Doxim, "to facilitate [its] Service ("Service Providers"), provide the Service on [its] behalf, perform Service-related services or assist [it] in analyzing how [its] Service is used. These third parties have access to [customers'] Personal Data only to perform these tasks on [its] behalf and are obligated not to disclose or use it for any other purpose."[9]

---

[6] *See* About Us, Triliant Federal Credit Union, https://www.truliantfcu.org/about-us (last visited June 12, 2024).
[7] *See Id.*
[8] Truliant Privacy Policy, Transfer of Data, https://www.truliantfcu.org/security-center/privacy-policy (last visited June 12, 2024).
[9] *Id*. Service Providers.

29. To protect its customers' personal information from unauthorized access and use, Truliant "use[es] security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[10]

30. Defendant Doxim was a third-party print and digital document and statement provider of Truliant. On its website, Doxim advertise itself as "a customer communications management and engagement-technology leader serving highly regulated organizations globally across the United States, Canada, the United Kingdom, and Africa. . . Today, Doxim is proud to partner with over 2,000 clients in highly regulated industries. Our software and managed services strengthen engagement across the customer lifecycle addressing key digitization, operational efficiency, and customer experience challenges."[11]

31. Doxim states on its website that "[t]he promise of security you provide to your customers – is our promise too. At Doxim, we take our responsibility to protect our clients' sensitive information very seriously. . . Doxim is proud to publish our 'A' verified security rating by Security Scorecard, a third party assessment of our security posture. Doxim ranked top across all criteria aligned with requirements and exceeding industry standards."[12]

32. In the regular course of their business, Defendants collect, store, and maintain the PII they receive from customers.

33. By creating and maintaining massive repositories of PII, Defendants have provided a particularly lucrative target for data thieves looking to obtain, misuse, or sell such data.

---

[10] Truliant Federal Credit Union Privacy Policy, https://www.truliantfcu.org/getmedia/1b18b65f-3c04-4fa2-9382-69230702044c/Privacy-Policy-as-of-08-2018.pdf (last visited June 12, 2024).
[11] About Us, Doxim, https://www.doxim.com/about-us/ (last visited June 12, 2024)
[12] Security Communications, Doxim, https://www.doxim.com/secure-communications/ (last visited June 12, 2024)

The Data Breach and Notice Letter

34. In or around February 2024, an unauthorized actor accessed computer systems in Defendant Doxim's network and obtained the PII of Plaintiff and Class Members. [13]

35. On or around April 22, 2024, Defendant Doxim notified Defendant Truliant of the Data Breach. Although Defendants claim that "[u]pon becoming aware of the issue, Doxim immediately began working with federal law enforcement and cybersecurity experts and have stated that the compromised files have been destroyed[]", they fail to o articulate what the investigation entailed.

36. On or around May 14, 2024, Defendant Truliant sent out a notice letter to Plaintiff and Class Members.[14] This means that Defendants waited approximately three months to notify the affected individuals.

37. According to information and belief, the Data Breach affected over 48,000 individuals.[15]

38. The information exposed or acquired as a result of the Data Breach is described by Truliant as "a combination of some of all of the following categories of information for each affected member: member name, account number, and Social Security number."[16] However, based on information and belief, Class Members' addresses and dates of birth are also impacted.[17]

39. To date, Defendants have not disclosed crucial information, including, but not limited to, the date and duration of the Data Breach; the exact extent of information that was collected by Defendants and exposed in the Data Breach; the identity of the hacking group

[13] *See supra* n.6.
[14] Notice Letter, *supra* n.5.
[15] *See supra* n.6.
[16] Notice Letter, *supra* n.5.
[17] *See supra* n.6.

responsible for the Data Breach; how the cybercriminals were able to exploit vulnerabilities in Defendants' IT security systems; the methodologies and full results of Defendants' investigation; any steps taken by Defendants to safeguard its systems other than simply destroying the compromised files.

40. Defendants' systems hacked by cybercriminals contained Plaintiff's and Class Members' PII that was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

41. Despite the ongoing and long-term risks for financial fraud and identity theft for victims of the Data Breach, Defendants do not offer sufficient identity protection services for the affected individuals. While Truliant offered free Equifax CreditWatch, this was only offered for 12 months and requires activation by the Dada Breach victims, which places a fraud alert on the victims' credit report, warning prospective lenders to take extra steps to verify the victims' identify before granting any credit. [18] This placed the burden on the Data Breach victims to spend time and effort to sign up for these services provided, and future hardship to obtain credit.

42. Plaintiff's and Class Members' PII was provided to Defendants, either directly or indirectly, with the reasonable expectation and mutual understanding that Defendants would comply with its obligation to keep such information confidential and secure from unauthorized access. Plaintiff and Class Members are harmed by such failure.

43. Defendants also benefited directly from the PII provided by Plaintiff and Class Members. As a financial service provider and a third-party print and digital document and statement provider, Defendants use the data they collect to perform their paid services to their customers.

[18] Notice Letter, *supra* n.7.

44. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

Defendants Knew That Criminals Target PII.

45. At all relevant times, Defendants knew or should have known that Plaintiff's and all other Class Members' PII was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyber-attacks that Defendants should have anticipated and guarded against.

46. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches preceding the date of the Data Breach, which has been widely reported in the last few years.

47. In the wake of the significant rise in data breaches, the Federal Trade Commission has also issued an abundance of guidance for companies and institutions that maintain individuals' PII.[19]

48. As a result of the notoriety of cyberattacks on systems like Defendants', several other government entities have also issued warnings to potential targets so that they may be alerted and prepared for a potential attack like the Data Breach.

[19] *See, e.g., Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N., https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited May 23, 2024).

49. The significant rise in data breaches have been a consistent problem for the past several years, providing Defendants sufficient time and notice to improve the security of its systems and engage in stronger, more comprehensive cybersecurity practices.

50. PII is a valuable property right.[20] The value of PII as a commodity is measurable.[21] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[22] American companies are estimated to have spent over $19 billion acquiring consumers' personal data in 2018.[23] In fact, it is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

51. As a result of its real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, and other PII directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFO. AND COMMC'N. TECH. 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . .").

[21] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[22] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[23] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

52. Consumers place a high value on the privacy of their PII. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[24]

53. Given these factors, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

54. Therefore, Defendants clearly knew or should have known of the risks of data breaches and thus should have ensured that adequate protections were in place, particularly given the nature of the PII stored in its unprotected files and the massive amount of PII it maintains.

Theft of PII has Grave and Lasting Consequences for Victims.

55. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victim's name, lock the victim out of their financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[25]

56. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[26] In addition, identity thieves

---

[24] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011), https://www.jstor.org/stable/23015560?seq=1.

[25] *See* Laura Pennington, *Recent Data Breach Trends Mean Your Info Was Likely Stolen Last Year*, TOP CLASS ACTIONS (Jan. 28, 2019), https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/.

[26] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes

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.[27]

57. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact on their credit.

58. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[28] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can adversely impact the victim's credit rating.

59. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[29]

"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." 12 C.F.R. § 1022.3(g).

[27] *See Warning Signs of Identity Theft*, FED. TRADE COMM'N, https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last visited May 16, 2024).

[28] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV'T ACCOUNTABILITY OFF. (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[29] *Id.* at 2, 9.

60. There may be a time lag between when PII is stolen and when it is used.[30] According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

61. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cybercriminals have openly posted stolen credit card numbers, Social Security Numbers, and other PII directly on various Internet websites, making the information publicly available.

62. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who companies employ to find flaws in their computer systems, stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[32]

---

[30] For example, on average, it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information. John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9, 12 (2019), https://www.iiisci.org/Journal/PDV/sci/pdfs/IP069LL19.pdf.

[31] U.S. GOV'T ACCOUNTABILITY OFF., *supra* n.22 at 29 (emphasis added).

[32] Patrick Lucas Austin, *'It is Absurd.' Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 P.M.), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

63. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft, and some need over a year.[33]

64. Plaintiff and Class Members must vigilantly monitor their financial accounts and their family members' accounts for many years to come. Indeed, as Ron Pierce, a Triad-based cyber expert commented regarding the Data Breach, "[f]or the customer, it just means that somebody, somewhere, may have some information about them that they could use against them[.]"[34]

65. It is within this context that Plaintiff and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

66. Plaintiff and all other Class Members have suffered injury and damages, including, but not limited to (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of

[33] *2021 Consumer Aftermath Report: How Identity Crimes Impact Victims, Their Families, Friends and Workplaces*, IDENTITY THEFT RES. CTR., https://www.idthecenter.org/identity-theft-aftermath-study/ (last visited May 16, 2024).

[34] Nixon Norman, Truliant reports customer data breach after third-party cyber security attack, May 29, 2024, https://www.wfmynews2.com/article/news/local/truliant-data-breach-2024/83-c8d8ca25-8133-4b32-b943-fc16a34258ee

the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

CLASS ALLEGATIONS

67. This action is brought and may be properly maintained as a class action pursuant to Rule 23(b)(2) and (3) of the Federal Rules of Civil Procedure.

68. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All persons whose PII was accessed in the Data Breach by unauthorized persons.

69. Plaintiff reserves the right to amend the above definition or to propose other or additional classes in subsequent pleadings and/or motions for class certification.

70. Plaintiff is a member of the Class.

71. Excluded from the Class are Defendants, their respective affiliates, parents, subsidiaries, officers, agents, directors, the judge(s) presiding over this matter, and the clerks of said judge(s).

72. This action seeks both injunctive relief and damages.

73. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

74. **Numerosity of the Class.** The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. Upon information and belief, there are over 48,000 Class Members in the Class. The exact number and identity of Class Members is readily identifiable in Defendants' records, which will be a subject of discovery.

75. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendants' data security systems prior to the Data Breach met the requirements of relevant laws;

b. Whether Defendants' data security systems prior to the Data Breach met industry standards;

c. Whether Defendants owed a duty to Plaintiff and Class Members to safeguard their PII;

d. Whether Defendants breached their duty to Plaintiff and Class Members to safeguard their PII;

e. Whether Defendants failed to provide timely and adequate notice of the Data Breach to Plaintiff and Class Members;

f. Whether Plaintiff's and Class Members' PII was compromised in the Data Breach;

g. Whether Plaintiff and Class Members are entitled to injunctive relief; and

h. Whether Plaintiff and Class Members are entitled to damages as a result of Defendants' conduct.

76. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and violations of law. Plaintiff and Class Members all had their PII stolen in the Data Breach. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendants.

77. **Adequacy of Representation.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

78. Plaintiff and his chosen attorneys -- Milberg Coleman Bryson Phillips Grossman, PLLC ("MCBPG"), and Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG", collectively, "Plaintiff's Counsel") -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint. In particular, Plaintiff's Counsel have respectively been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. Plaintiff's Counsel are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, Plaintiff's Counsel possess the financial resources necessary to ensure that a lack of financial capacity will not hamper the litigation and is willing to absorb the costs of the litigation.

79. **Predominance.** The common issues identified above arising from Defendants' conduct predominate over any issues affecting only individual Class Members. The common issues hinge on Defendants' common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

80. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large number of injured persons, to keep the courts from becoming paralyzed by a multitude of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

81. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which, in any event, might cause inconsistent results.

b. When the liability of Defendants have been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class Members, in terms of monetary damages due and terms of equitable relief, can be determined in this single proceeding rather than in multiple individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendants, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only customers of Defendants, the legal and factual issues are narrow and easily defined, and the Class Membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendants' records, such that direct notice to the Class Members would be appropriate.

82. **Injunctive relief.** Defendants have acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final injunctive or equitable relief on a class-wide basis.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class Against Both Defendants)

83. Plaintiff realleges and incorporates by reference paragraphs 1 through 82 as if fully set forth herein.

84. To perform its financial services, Defendant Truliant collects Plaintiff's and Class Members' PII from its customers, and provides the PII to Defendant Doxim for its third-party print and digital document and statement services.

85. By collecting and storing their PII and using it for commercial gain, at all times relevant, Defendants owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

86. Defendants owed a duty of care to Plaintiff and Class Members to provide data security consistent with statutory and industry standards and to ensure that its systems and networks and the personnel responsible for them adequately protected the PII.

87. Defendants knew the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems. Defendants knew of the many data breaches that targeted companies that store PII in recent years.

88. Given the nature of Defendants' businesses, the sensitivity and value of the PII it maintains, and the resources at its disposal, Defendants should have identified the vulnerabilities in their systems and prevented the Data Breach from occurring.

89. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them -- including Plaintiff's and Class Members' PII.

90. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of customers that Defendants were aware, or should have been aware, could be injured by inadequate data security measures.

91. Plaintiff and Class Members have no ability to protect their PII that was or remains in Defendants' possession.

92. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

93. But for Defendants' negligent conduct and breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

94. Defendants' conduct was grossly negligent and departed from reasonable standards of care, including but not limited to failing to adequately protect Plaintiff's and Class Members' PII and failing to provide them with timely notice that their PII had been compromised.

95. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

96. By failing to provide timely and complete notification of the Data Breach to Plaintiff and Class Members, Defendants prevented them from proactively taking steps to secure their PII and mitigate the associated threats.

97. As a result of Defendants' above-described wrongful actions, inaction, and lack of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered and will continue to suffer economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled

to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class Against Both Defendants)

98. Plaintiff realleges and incorporates by reference paragraphs 1 through 82 as if fully set forth herein.

99. Defendants had duties by statute to ensure that all information they collected and stored was secure and that they maintained adequate and commercially reasonable data security practices to ensure the protection of Plaintiff's and Class Members' PII.

100. Defendants' duties arise from, *inter alia*, Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

101. The FTC has published numerous guides for businesses that highlight the importance of implementing reasonable data security practices. In 2016, the FTC updated its publication establishing cybersecurity guidelines for businesses, which makes thorough recommendations, including, but not limited to, for businesses to protect the personal customer information they keep, 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 any security problems.[35]

102. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, 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 FTCA. Orders resulting from these actions further clarify the measures businesses such as Defendants must take to meet their data security obligations and effectively put Defendants on notice of these standards.

103. Defendants violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all Class Members' PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtains and stores and the foreseeable consequences of a data breach involving PII, including, specifically, the substantial damages that would result to Plaintiff and other Class Members.

104. Defendants' violation of the FTCA constitutes negligence per se.

105. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA was intended to protect.

106. The harm occurring as a result of the Data Breach is the type of harm against which Section 5 of the FTCA was intended to guard.

107. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security

[35] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N. (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

108. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violation of Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft and medical identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

109. Defendants' violation of the FTCA constitutes negligence *per se* for purposes of establishing the duty and breach elements of Plaintiff's negligence claim. Those statutes were designed to protect a group to which Plaintiff belongs and to prevent the type of harm that resulted from the Data Breach.

110. Defendants owed a duty of care to Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

111. It was foreseeable that Defendants' failure to use reasonable measures to protect PII and provide timely notice of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

112. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class Against Defendant Truliant)

113. Plaintiff realleges and incorporates by reference paragraphs 1 through 82 as if fully set forth herein.

114. Plaintiff's and Class Members' PII was provided to Truliant in confidence, believing that Truliant would protect that information. Truliant's customers would not have provided Truliant with this information had they known they would not be adequately protected. Truliant's acceptance and storage of Plaintiff's and Class Members' PII created a fiduciary relationship between Truliant and Plaintiff and Class Members.

115. In light of this relationship, Truliant have a fiduciary duty to act for the benefit of its customers and Plaintiff and Class Members upon matters within the scope of their relationship, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

116. Truliant breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII and otherwise failing to safeguard Plaintiff's and Class Members' PII that it collected.

117. As a direct and proximate result of Truliant's breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer injury, including, but not limited to (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) the improper compromise, publication, and theft of their PII; (iii) deprivation of the value of their PII, for which there is a well-established national and international market; (iv) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (v) the continued risk to their PII which remains in Truliant's possession.

COUNT IV
BREACH OF CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant Truliant)

118. Plaintiff realleges and incorporates by reference paragraphs 1 through 82 as if fully set forth herein.

119. Defendant Truliant entered into various written contracts with Plaintiff and Class Members to perform services that include, but are not limited to, financial services.

120. These contracts were made in part for the benefit of Plaintiff and the Class. Indeed, Defendant Truliant knew that if it were to breach these contracts with its customers, its customers, including Plaintiff and Class Members, would be harmed by, among other things, fraudulent misuse of their PII.

121. It was intended by Defendant Truliant at the time the contracts were made that Defendant Truliant would assume a direct obligation to protect Plaintiff's and the Class's PII.

122. It was also intended by Defendant Truliant that the performance under the contract would necessarily and directly benefit Plaintiff and the Class. Defendant Truliant would utilize the PII it collected in providing timely and accurate financial services to its customers.

123. Defendant Truliant breached its contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' PII in a manner that complies with applicable laws, regulations, and industry standards, and resulting compromise of Plaintiff's and Class Members' PII.

COUNT V
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of Plaintiff and the Class Against Defendant Doxim)

124. Plaintiff realleges and incorporates by reference paragraphs 1 through 82 as if fully set forth herein.

125. Defendant Doxim entered into a written contract with Defendant Truliant to perform services that include, but are not limited to, print and digital document and statement services.

126. This contract was made in part for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contract entered into between Defendants. Indeed, Defendants knew that if they were to breach the implied contract with the Truliant's customers, Truliant's customers, including Plaintiff and Class Members, would be harmed by, among other things, fraudulent misuse of their PII.

127. It was intended by Defendant Doxim at the time the contracts were made that Defendant Doxim would assume a direct obligation to protect Plaintiff's and the Class's PII.

128. It was also intended by Defendant Doxim that the performance under the contract would necessarily and directly benefit Plaintiff and the Class. Defendant Doxim would utilize the PII it collected in providing timely and accurate print and digital document and statement services for Plaintiff and Class Members, on behalf of Truliant.

129. Defendant Doxim breached its obligations under its implied contracts, to which Plaintiff and Class Members are intended beneficiaries, directly resulted in the Data Breach and the injuries that Plaintiff and all other Class Members have suffered.

130. As a direct and proximate result of Defendants' breach of implied contracts, Plaintiff and all other Class Members suffered and will continue to suffer damages, because (i) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) their PII was improperly disclosed to unauthorized individuals; (iii) the confidentiality of their PII has been breached; (iv) they were deprived of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred, and future costs required, to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT VI
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class Against Both Defendants)

131. Plaintiff realleges and incorporates by reference paragraphs 1 through 82 as if fully set forth herein.

132. Plaintiff brings this claim, on behalf of himself and the Class, in the alternative to all other claims and remedies at law.

133. Defendant Turliant was conferred a monetary benefit upon by collecting Plaintiff's and Class Members' PII, in the forms of (1) monies paid for services by Plaintiff and Class Members, and (2) the provision of Plaintiff's and Class Members' valuable PII. Indeed, upon acquiring the PII, Defendant Turliant was then able to charge money for its services and utilize the PII for several purposes, including but not limited providing its services, conducting consumer research, billing, and contacting customers. The PII was thus used to facilitate payment and generate additional revenue for Defendant Turliant.

134. Defendant Doxim was conferred a monetary benefit upon by collecting Plaintiff's and Class Members' PII, in the forms of (1) monies paid for services by Turliant, and (2) the provision of Plaintiff's and Class Members' valuable PII. Indeed, upon acquiring the PII, Defendant Doxim was then able to charge money for its services from Truliant and utilize the PII. The PII was thus used to facilitate payment and generate additional revenue for Defendant.

135. Defendants accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Defendants profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

136. Upon information and belief, Defendants, like most other corporate entities, funds its data security measures entirely from its general revenue, which includes money paid by Plaintiff and Class Members.

137. As such, a portion of the payments made for Defendants' services are or should have been used to provide a reasonable level of data security.

138. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure the PII it collects.

139. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants avoided their data security obligations at the expense of Plaintiff and Class Members by utilizing less expensive and less effective security measures.

140. As a direct and proximate result of Defendants' failure to provide the requisite security, Plaintiff and Class Members suffered actual damages.

141. Defendants should not be permitted to retain the money profited by collecting PII of Plaintiff and Class Members because Defendants failed to adequately implement the data privacy and security procedures mandated by federal, state, and local laws and industry standards.

142. Defendants should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it as a result of its conduct and the resulting Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendants as follows:

A. Certifying that Class as requested herein, appointing the named Plaintiff as Class representative and the undersigned counsel as Class Counsel;

B. Requiring that Defendants pay for notifying the members of the Class of the pendency of this suit;

C. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

D. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendants from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend additional credit monitoring services and similar services to protect against all types of identity theft and medical identity theft.

E. Awarding Plaintiff and the Class prejudgment and post-judgment interest to the maximum extent allowable;

F. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable, together with their costs and disbursements of this action; and

G. Awarding Plaintiff and the Class such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: June 13, 2024

Respectfully submitted,

/s/ Scott C. Harris
Scott C. Harris
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan St.
Raleigh, NC 27603
Telephone: (919) 600-5003
sharris@milberg.com

Todd S. Garber (*Pro Hac Vice application forthcoming*)
FINKELSTEIN, BLANKINSHIP
FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com

Attorneys for Plaintiff and the Proposed Class

ClassAction.org
