IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MICHIGAN

THOMAS WARDROP, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	
v.	)	Case No.:
CREDIT UNION ONE and DOXIM, INC.,	)	JURY TRIAL DEMANDED
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Thomas Wardrop ("Plaintiff"), on behalf of himself and all others similarly situated, through his undersigned counsel complains against Defendants Credit Union ONE and Doxim, Inc. ("Doxim") (collectively, "Defendants") 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. Credit Union ONE is a Michigan state-chartered credit union that provides financial services to its members. Credit Union ONE contracted with Doxim for print and digital document and statement services.

3. Doxim collected and maintained sensitive PII of Credit Union ONE's depositors for the purpose of providing print and digital document and statement services.

4. On or about December 30, 2023, an unauthorized actor gained access to Doxim's network and computer systems and obtained unauthorized access to Defendants' files. As a result

of the acts and omissions of Defendants alleged herein, cybercriminals were able to gain access to Defendants' data records and access sensitive and valuable PII of Plaintiff and Class Members (the "Data Breach").

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. On information and belief, information disclosed in the Data Breach includes but is not limited to Class Members' names, mailing addresses, Social Security numbers, account numbers, and other financial information.

6. On its website, Credit Union ONE states, "To protect Personal Information from unauthorized access and use, we use security measures that comply with applicable federal and state laws. These measures may include device safeguards and secured files and buildings as well as oversight of our third party service providers to ensure information remains confidential and secure."[1]

7. According to the notice letter from Doxim to Credit Union ONE's customers, dated May 31, 2024, "[A] recent security incident at Doxim Inc., . . . resulted in unauthorized access to files containing your personal information. Doxim is a third-party service provider that has assisted Credit Union ONE with the preparation of account statements and/or income tax forms for its members."[2] [3]

8. Further, according to Doxim's Notice Letter, "On December 30, 2023, Doxim detected suspicious activity within the portion of its computer network supporting its credit union services. . . . As part of our investigation, we determined that files had been removed from our

[1] *Online Privacy*, CREDIT UNION ONE, https://www.cuone.org/resources/helpful-links/security-center/online-privacy (last visited Oct. 9, 2024).

[2] Notice of Security Incident from Mike Hennessy to Thomas Wardrop (May 31, 2024) (hereinafter "Notice Letter") (attached as Exhibit A).

[3] A complete copy of the form letter sent to Plaintiff and other Class members is attached hereto as Exhibit B.

network. Following an in-depth review of those files, we recently discovered that some of those files included your personal information."[4]

9. As a result of Defendants' failure to protect the PII they were entrusted to safeguard, Plaintiff and Class Members suffered a loss of the value of their PII 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.

10. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes, including opening new financial accounts 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.

11. 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.

12. 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.

13. 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

[4] *Id.*

must now and in the future closely monitor their financial accounts to guard against identity theft.

14. 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 Defendants.

15. Plaintiff, on behalf of himself and all other Class Members, asserts claims for negligence, negligence *per se*, breach of fiduciary duty, breach of contract, breach of third-party beneficiary 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

16. Plaintiff, Thomas Wardrop, is a natural person and domiciliary of Grand Rapids, Michigan. Mr. Wardrop is a member of the Class defined herein.

17. Plaintiff received a Notice Letter from Defendant Doxim dated May 31, 2024, detailing that, as a member of Defendant Credit Union ONE, his data had been compromised.[5] The Notice Letter advised that files containing Plaintiff's PII had been removed from Doxim's network as part of the Data Breach.[6]

18. 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 Credit Union ONE. Doxim collects and stores PII to perform its services for Credit Union ONE. Plaintiff does not have any ability to protect his PII that was or remains in Defendants' possession.

[5] *Id.*
[6] *Id.*

19. Defendant Credit Union ONE is a Michigan state-chartered credit union with its principal place of business in Ferndale, Michigan. In the regular course of its business, Defendant Credit Union ONE takes custody of and maintains control over PII from its customers.

20. 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 Michigan and takes custody of and maintains control over PII from Credit Union ONE's customers, including Plaintiff and Class Members.

JURISDICTION AND VENUE

21. 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 interest and costs.

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

23. This Court has personal jurisdiction over Defendant Doxim because Defendant Doxim has sufficient minimum contacts in the State, and Defendant Doxim engaged in the conduct underlying this action in Michigan, including the collection, storage, and inadequate safeguarding

of Plaintiff's and Class Members' PII. Defendant Doxim intentionally availed itself of this jurisdiction by marketing and selling services and accepting and processing payments for those services within Michigan.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant Credit Union ONE 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

25. Defendant Credit Union ONE is a Michigan state-chartered credit union that provides financial services to individuals and businesses, including banking services, investment services, financial planning, and insurance.[7] Credit Union ONE was chartered in 1938 and currently serves over 112,000 members with 17 branches in Metro Detroit, Grand Rapids, and Traverse City and over $1.7 billion in assets.[8]

26. On its website, Credit Union ONE states, "Our top priority is your security," and further assures that Credit Union ONE's "policies are designed to safeguard your personal information and financial data."[9]

27. Credit Union ONE contracts with third party companies and individuals, including Defendant Doxim, in the regular course of its business to, for example, "process [member] transactions" and "maintain [member] account(s)."[10]

---

[7] *Services*, CREDIT UNION ONE, https://www.cuone.org/ (last visited Oct. 9, 2024).

[8] *About Us*, CREDIT UNION ONE, https://www.cuone.org/about/about-us (last visited Oct. 9, 2024); *Credit Union Details*, NAT'L CREDIT UNION ADMIN., https://mapping.ncua.gov/CreditUnionDetails/62562 (last visited Oct. 9, 2024).

[9] *Security Center*, CREDIT UNION ONE, https://www.cuone.org/resources/helpful-links/security-center (last visited Oct. 9, 2024).

[10] *Privacy Statement*, Credit Union ONE (May 2023), chrome-

28. To protect its customers' personal information from unauthorized access and use, Credit Union ONE purportedly "use[s] security measures that comply with applicable federal and state laws. These measures may include device safeguards and secured files and buildings as well as oversight of [Credit Union ONE's] third party service providers to ensure information remains confidential and secure."[11]

29. Defendant Doxim was a third-party print and digital document and statement provider of Credit Union ONE. On its website, Doxim advertises 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."[12]

30. 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."[13]

31. In the regular course of their business, Defendants collect, store, and maintain the

---

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cuone.org/getmedia/0027cd68-9ba6-4eb5-84b0-6cafdb7ca61c/5-23-23-Privacy-Notice-without-Opt-OUT-02100911-DXPS0-C-1-050123-DXPS01-E-_CUF.pdf.

[11] *Credit Union ONE Online Privacy Policy*, CREDIT UNION ONE, https://www.cuone.org/resources/helpful-links/security-center/online-privacy (last visited Oct. 9, 2024).

[12] *About Us*, Doxim, https://www.doxim.com/about-us/ (last visited Aug. 27, 2024).

[13] *Security Communications*, Doxim, https://www.doxim.com/secure-communications/ (last visited Aug. 27, 2024).

PII they receive from customers.

32. 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.

The Data Breach and Notice Letter

33. In or around December 2023, an unauthorized actor accessed computer systems in Defendant Doxim's network and obtained the PII of Plaintiff and Class Members.[14]

34. In or around April of 2024, Defendant Doxim notified several affected credit unions, including Credit Union ONE, of the Data Breach.

35. On or around May 31, 2024, Defendant Doxim sent a Notice Letter to Plaintiff and Class Members.[15] Upon information and belief, Defendant Credit Union ONE has, to date, failed to provide any notice of the Data Breach to its customers. This means that Defendant Doxim waited approximately five months to notify the affected individuals, and Defendant Credit Union ONE has yet to notify affected customers.

36. Although Defendant Doxim claims that "[u]pon discovering the situation, we promptly took these systems offline, notified law enforcement, and engaged industry-leading cybersecurity experts to investigate," they fail to articulate what the investigation entailed.[16]

37. Upon information and belief, the Data Breach affected tens of thousands of individuals.[17]

38. The information exposed or obtained from Doxim's network as a result of the Data

[14] Notice Letter, *supra* note 2.
[15] *Id.*
[16] *Id.*
[17] Credit Union ONE has assets of over $1.7 billion, which include the deposits of its members. See 2023 Annual Report (available at https://www.cuone.org/getmedia/d74bb3a7-47d6-41e9-a408-7f386fe2cf89/2023-Annual-Report.pdf) (last accessed Oct. 9, 2024).

Breach include consumers' "name, mailing address, account number, and/or Social Security number."[18]

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 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; and any steps taken by Defendants to safeguard its systems.

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. Doxim has offered complimentary Kroll Identity Monitoring Services lasting only 12 months and requiring activation by the Data Breach victims. This places the burden on the Data Breach victims to spend time and effort to sign up for these services and fails to address the threat of identity theft and financial fraud Data Breach victims face for years to come.

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 Defendants' failure to maintain the security and confidentiality of the sensitive PII Plaintiff and Class Members entrusted to them.

[18] *Id.*

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.

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 cyberattacks 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

[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 Oct. 9, 2024).

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.

49. The significant rise in data breaches has 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

---

[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/.

aggregated and become more valuable to thieves and more damaging to victims.

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.

Defendants Failed to Comply with FTC Guidelines

55. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable and adequate data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

56. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[25] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[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 Protecting Personal Information: A Guide for Business*, *supra* note 18.

networks; understand their networks' vulnerabilities; and implement policies to correct any security problems.[26] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[27]

57. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[28]

58. The FTC has brought enforcement actions against businesses for failing to protect 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.

59. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

---

[26] *Id.*

[27] *Id.*

[28] *Start with Security: A Guide for Business,* FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 9, 2024).

60. To prevent and detect cyber-attacks, including the cyber-attack on Defendants' network that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government and FTC, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of malware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices using a centralized patch management system;

f. Set anti-virus and anti-malware programs to automatically conduct regular scans and/or repairs;

g. Create and manage the use of privileged accounts based on the varying level of accessibility using a principle of least privilege: wherein no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary, such as any internal IT employees;

h. Configure access controls—including file, directory, and network share

permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common malware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

61. Defendants were at all times fully aware of their obligation to protect the PII of their clients' customers, prospective customers, and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

62. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices. Best cybersecurity practices that are standard in the financial services

industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points of security.

63. Upon information and belief. Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1[29] (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[30] (CIS CSC), which are all established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyberattack and causing the Data Breach.

64. The occurrence of the Data Breach is indicative that Defendants failed to adequately implement one or more of the above measures to prevent or circumvent ransomware attacks or other forms of malicious cybercrimes, resulting in the Data Breach.

Theft of PII has Grave and Lasting Consequences for Victims.

65. 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:

---

[29] Nat'l Inst. of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (2018), *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[30] *See The 18 CIS Critical Security Controls*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/cis-controls-list (last visited May 11, 2023).

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.[31]

66. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[32] In addition, identity thieves may obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[33]

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

68. 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.[34] 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

---

[31] *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/.

[32] 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 "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).

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

[34] *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.

adversely impact the victim's credit rating.

69. 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."[35]

70. There may be a time lag between when PII is stolen and when it is used.[36] 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.[37]

71. 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.

72. 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. Noted data security researcher Tom Stickley, who is frequently employed to find security flaws in corporate computer systems, has said, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy

---

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

[36] 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.

[37] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 33 at 29 (emphasis added).

pickings."[38]

73. 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.[39]

74. 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[.]"[40]

75. 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

76. Defendants have failed to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

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

---

[38] 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/.

[39] *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).

[40] Nixon Norman, *Truliant reports customer data breach after third-party cyber security attack,* WFMY NEWS 2 (May 29, 2024), https://www.wfmynews2.com/article/news/local/truliant-data-breach-2024/83-c8d8ca25-8133-4b32-b943-fc16a34258ee.

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

79. Plaintiff and Class Members have been and currently face substantial risk of being targeted now and in the future for phishing schemes, data intrusion, and other illegality based on their PII being compromised in the Data Breach as potential fraudsters could use the information garnered to target such schemes more effectively against Plaintiff and Class Members.

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

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

82. Plaintiff and Class Members have spent and will continue to spend significant amounts of uncompensated time to monitor their financial accounts, medical accounts, sensitive information, credit score, and records for misuse.

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

84. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of proper and adequate security measures and safeguards, including but not

limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

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

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

87. Plaintiff and Class Members have suffered injury and damages, 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) 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.

Plaintiff Thomas Wardrop's Experience

88. As a condition of receiving banking and related services, Plaintiff entrusted his PII and other confidential information to Credit Union ONE and its statement services vendor, Doxim, with the reasonable expectation and understanding that they and their agents would take industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to his PII. Plaintiff would not have so entrusted his PII to Defendants had he known that it was not

securely stored or that they would not take reasonable steps to safeguard his PII.

89. On or about May 31, 2024, Plaintiff Wardrop received a Notice Letter from Defendant Doxim, which informed him of the Data Breach and that he faced a substantial and significant risk of his PII being misused. The Notice informed Plaintiff that his PII had been improperly access and obtained by unauthorized third parties. The Notice indicated that Plaintiff's PII was compromised as a result of the Data Breach.

90. Plaintiff Wardrop is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Wardrop stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

91. Plaintiff has been forced to spend time dealing with the direct consequences of the Data Breach and making reasonable efforts to mitigate the impact of the Data Breach, which include spending time researching the Data Breach, researching credit monitoring and identity theft protection services, reviewing various financial statements and accounts, and monitoring his credit. This is uncompensated time that has been lost forever and cannot be recaptured.

92. Plaintiff Wardrop has spent significant time responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

93. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of his PII—a form of intangible property that Plaintiff entrusted to Defendants. This PII was compromised in, and has been diminished as a result of, the Data Breach.

94. Plaintiff Wardrop suffered actual injury from having his sensitive PII exposed and stolen as a result of the Data Breach including, but not limited to: (a) actual fraud and identity theft; (b) entrusting

PII to Defendants that he would not have had Defendants disclosed they lacked data security practices adequate to safeguard its customers' PII; (c) damages to and diminution in the value of his PII–a form of intangible property that he entrusted to Defendants as a condition of receiving financial services; (d) loss of his privacy; (e) continuous imminent and impending injury arising from the increased risk of financial and identity fraud and theft; and (f) time and expense of his mitigation efforts as a result of the Data Breach.

95. Plaintiff Wardrop has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his name, which is now in the hands of cyber criminals and other unauthorized third parties.

96. Knowing that thieves stole his PII, including his Social Security number, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff to experience feelings of rage, anger, anxiety, sleep disruption, stress, and fear. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

97. Plaintiff has a continuing interest in ensuring that his PII, which upon information and belief, remains in the possession of Defendants, is protected and safeguarded from future data breaches.

98. As a result of the Data Breach, Plaintiff is presently and will continue to be at a heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages for years to come.

CLASS ALLEGATIONS

99. 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.

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

> All persons whose PII was impacted by the Data Breach, including all persons to whom Defendants sent a notice of the Data Breach.
>
> *Credit Union ONE Subclass*
>
> All persons in the above-defined class who are or were also members of Credit Union ONE.

101. 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.

102. Plaintiff is a member of the Class and Subclass defined above.

103. 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).

104. This action seeks both injunctive relief and damages.

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

106. **Numerosity.** The exact number of members of the Class is unknown but, upon information and belief, it is estimated to number in the tens or hundreds of thousands at this time, and individual joinder in this case is impracticable. Members of the Class can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

107. **Commonality.** 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.

108. **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.

109. **Adequacy.** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained the undersigned counsel who are competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiff.

110. **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.

111. **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.

112. 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 has 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.

113. **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)

114. Plaintiff realleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

115. To perform its financial services, Defendant Credit Union ONE 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.

116. 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.

117. 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.

118. 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.

119. 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.

120. 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.

121. 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.

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

123. 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.

124. 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.

125. 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.

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

127. 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.

128. 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 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 financial fraud—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)

129. Plaintiff realleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

130. 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.

131. 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.

132. 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.[41]

133. 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.

134. 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.

[41] *Protecting Personal Information: A Guide for Business*, *supra* note 18.

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

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

137. 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.

138. 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 release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

139. 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 financial fraud—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.

140. 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.

141. 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.

142. 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.

143. 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 Credit Union ONE)

144. Plaintiff realleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

145. Plaintiff's and Class Members' PII was provided to Credit Union ONE in confidence, believing that Credit Union ONE would protect that information. Credit Union ONE's

customers would not have provided Credit Union ONE with this information had they known they would not be adequately protected. Credit Union ONE's acceptance and storage of Plaintiff's and Class Members' PII created a fiduciary relationship between Credit Union ONE and Plaintiff and Class Members.

146. In light of this relationship, Credit Union ONE has 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.

147. Credit Union ONE 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.

148. As a direct and proximate result of Credit Union ONE'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 and financial fraud—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 Credit Union ONE's possession.

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

149. Plaintiff realleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

150. Defendant Credit Union ONE entered into various written contracts with Plaintiff and Class Members to perform services that include, but are not limited to, financial services.

151. These contracts were made in part for the benefit of Plaintiff and the Class. Indeed, Defendant Credit Union ONE 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.

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

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

154. Defendant Credit Union ONE 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)

155. Plaintiff realleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

156. Defendant Doxim entered into a written contract with Defendant Credit Union

ONE to perform services that include, but are not limited to, print and digital document and statement services.

157. 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 Credit Union ONE's customers, Credit Union ONE's customers, including Plaintiff and Class Members, would be harmed by, among other things, fraudulent misuse of their PII.

158. 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.

159. 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 Credit Union ONE.

160. 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.

161. 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 and financial fraud—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)

162. Plaintiff realleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

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

164. Defendant Credit Union ONE 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 Credit Union ONE 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 Credit Union ONE.

165. 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 Credit Union ONE, 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 Credit Union ONE and utilize the PII. The PII was thus used to facilitate payment and generate additional revenue for Defendant.

166. 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.

167. 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.

168. 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.

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

170. 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.

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

172. 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.

173. 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: October 11, 2024

Respectfully submitted,

/s/ William M. Sweetnam

William M. Sweetnam (Bar No. IL6226203)
Laura Edmondson (*pro hac vice*)
JOHNSON FIRM
610 President Clinton Avenue, Suite 200
Little Rock, Arkansas 72201
(501) 777-7777
bill@yourattorney.com
laura@yourattorney.com

Attorneys for Plaintiff and the Proposed Class