UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
NEWPORT NEWS DIVISION

JORDAN HAMILTON, on behalf of herself, and all others similarly situated, ***Plaintiff*** **v.** **R&B CORPORATION OF VIRGINIA D/B/A CREDIT CONTROL CORPORATION** ***Defendant***	**Civil Action No. 4:23-cv-76**

CLASS ACTION COMPLAINT

Plaintiff, JORDAN HAMILTON (hereinafter, "Plaintiff"), on behalf of herself, and all others similarly situated, for her causes of action against the Defendant, R & B CORPORATION OF VIRGINIA d/b/a CREDIT CONTROL CORPORATION ("Defendant" or "CCC"), alleges upon personal knowledge as to her own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This action arises out of Defendant's unauthorized disclosure of the confidential personal information, Personally Identifying Information[1] ("PII") and Protected Health

[1] The Federal Trade Commission defines "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." 17 C.F.R. § 248.201(b)(8).

Information ("PHI")[2] (collectively, "PII"), of Plaintiff and the proposed Class Members, approximately 286,699 individuals, from March 2, 2023 to March 7, 2023 in a cyberattack on CCC's systems, including their names, addresses, Social Security numbers, and information relating to their accounts with Defendant's business partners such as account number, account balance, and date of service (the "Data Breach").[3]

2. CCC is a company headquartered in Newport News, Virginia, which performs debt collection services, including for medical offices, hospital systems, "small cable service[s, and] massive utility provider[s]."[4]

3. In connection with performing these debt collection services, CCC collects massive amounts of PII regarding its clients' customers, including Plaintiff and the Class Members.

---

[2] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last accessed Apr. 16, 2020). On information and belief, CCC is a "Business Associate" under HIPAA and some of the data compromised in the Data Breach that this action arises out of is "protected health information," subject to HIPAA.

[3] *See*: Credit Control Corporation—Notice of Data Incident available at https://creditcontrol.net/notice-of-data-incident/ **attached as Exhibit A;** "Credit Control Corporation - Notice of Data Event - ME.pdf," to Maine Attorney General, including sample data breach notice ("Data Breach Notice") available at file:///C:/Users/AndrewMize/OneDrive%20-%20Stranchlaw/credit%20control%20corporation/Credit%20Control%20Corporation%20-%20Notice%20of%20Data%20Event%20-%20ME.pdf , **attached as Exhibit B.**

[4] *See* https://creditcontrol.net/services/

4. On information and belief, CCC failed to undertake adequate measures to safeguard the PII of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

5. Although CCC discovered the Data Breach on or about March 7, 2023, Defendant failed to notify and warn Data Breach victims of the unauthorized disclosure of their PII until May 15, 2023.

6. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive PII and warn them promptly and fully about the Data Breach, they have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

PARTIES

7. Plaintiff is a natural person, and resident and citizen of the Commonwealth of Virginia with a primary residence in Locust Dale, Virginia, in Madison County where she intends to remain, and a victim of Defendant's Data Breach.

8. CCC is a corporation organized and existing under the laws of the Commonwealth of Virginia with a principal place of business located at 11821 Rock Landing Drive, Newport News, Virginia.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business in this state; it maintains its principal place of business and headquarters in Virginia; and committed tortious acts in Virginia.

10. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the class is a citizen of a state different from Defendant.

11. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

12. Venue is proper under 28 U.S.C. § 1391(b)(1) and (2) because Defendant resides in this district and a substantial part of the events and omissions giving rise to Plaintiff's claims occurred in this district.

FACTUAL BACKGROUND

A. Defendant CCC

13. Founded in 1953 and based in Newport News, Virginia, CCC is a company that provides debt collection services to clients, "specializing in healthcare, utility, and commercial collections."[5]

14. CCC provides debt collection services for numerous entities, including Sentara Health System, Riverside Health System, UVA Health System, Bayview Physicians Group, Pariser Dermatology Specialists, Inc, Valley Health System, Dominion Pathology Laboratories, Chesapeake Radiology, Children's Hospital of the King's Daughters Health System and its Affiliates, VCU Health System, Chesapeake Regional Medical Center, Mary Washington Healthcare, Urology of Virginia, Fauquier Health System, and Tidewater Physicians Multispecialty Group.[6]

[5] https://creditcontrol.net/services/ ; https://creditcontrol.net/about-us/compliance/
[6] See Notice of Data Incident, Exhibit A.

15. As a condition of these providing debt collection services, CCC requires that its partners provide their customers' and debtors' PII, including names, addresses, Social Security numbers, and information relating to their accounts such as account number, account balance, and dates of service.

16. In exchange for this information, CCC promises to safeguard its clients' customers' PII, and to only use this confidential information for authorized purposes.

17. Defendant acknowledges the importance of properly safeguarding the private data and PII of individuals, stating on its website that, "we further pledge to remain compliant with FDCPA, FCRA, HIPAA, PCI, FTC, UDAAP, and GLBA regulations pertaining to debt collection operations and, to educate/train and monitor our employees accordingly."[7]

18. As Defendant's website goes onto say:

> To provide even more assurance, an independent firm conducts an annual SOC audit to attest that CCC's internal controls are suitably designed and operating effectively. With these safeguards and a $5M cyber-liability insurance policy, our clients can take comfort that customers' protected information (PHI) is safe on our network.[8]

19. Plaintiff and the proposed Class Members, current and former customers of CCC's partners, would not have allowed their PII to be entrusted to Defendant had they known CCC would not adequately safeguard that information.

20. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and the proposed Class Members' PII, Defendant assumed legal and equitable duties to Plaintiff, and the members of the Proposed Class, and knew or should have known that it was responsible for protecting her and their PII from unauthorized disclosure.

---

[7] https://creditcontrol.net/about-us/
[8] Id.

21. At all times Plaintiff and the members of the Proposed Class, have taken reasonable steps to maintain the confidentiality of their PII; and, Plaintiff and the proposed Class Members, relied on Defendant to keep their PII confidential and securely maintained.

B. CCC Fails to Adequately Safeguard PII—the Data Breach

22. Plaintiff and the proposed Class Members are current and former customers of partners and vendors of Defendant, CCC, whose personal information, PII, was entrusted to CCC, directly or indirectly, in connection with Defendant's debt collection services.

23. CCC collected and maintained this PII in its computer information technology systems and networks.

24. From March 2, 2023 to March 7, 2023, CCC experienced a cyberattack to its systems in which the PII of its partners' and vendors' customers, including Plaintiff and the proposed Class Members, was unauthorizedly disclosed, including their names, addresses, Social Security Numbers, and information relating to the individual's accounts with CCC's business partners such as account number, account balance, and date of service—the Data Breach.[9]

25. On May 13, 2023, CCC posted the Notice of Data Incident, Exhibit A, on its website, and on or about May 15, 2023 began notifying affected consumers in writing ("Data Breach Notice, Exhibit B").[10]

26. According to Defendant's Notice of Data Incident (Ex. A) and Data Breach Notice (Ex. B), on March 7, 2023, CCC discovered "unusual activity involving certain systems within CCC's network," after which it "isolated the systems, and, with the assistance of third-party forensic specialists, commenced a comprehensive investigation into the nature and scope of the

[9] *See* Notice of Data Incident, **Exhibit A.**
[10] *See* notification to Maine Attorney General and sample Notice of Data Security Incident ("Data Breach Notice"), **Exhibit B.**

activity."[11]

27. Further according to Defendant, as of March 14, 2023, CCC had determined that from March 2, 2023 to March 7, 2023, "certain files were copied from CCC's network," after which Defendant "undertook a thorough review of the files in order to identify what specific information was present in the files and to whom it related."[12]

28. On information and belief, as CCC stated in the Data Breach Notice, Defendant then implemented addition security measures to secure the information in its systems, increased the frequency of employee training, notified its business partners, and notified law enforcement.[13]

29. In its notices, CCC encouraged affected persons to "remain vigilant against incidents of identity theft and fraud by reviewing [their] account statements and monitoring [their] free credit reports for suspicious activity," as well as apprising them of their ability to place a fraud alert on their credit files and a credit freeze on their credit reports.[14]

30. CCC offered victims of the Data Breach identity monitoring services through Kroll for one (1) year.[15]

31. On or about May 15, 2023, CCC reported the Data Breach to the Maine Attorney General, describing the Data Breach as an, "[e]xternal system breach (hacking)" event; that 286,699 persons were affected; that the Data Breach was discovered on May 3, 2023; that persons' names and Social Security Numbers were acquired; and that consumers were being notified on May 15, 2023.[16]

---

[11] Notice of Data Security Incident, Exhibit A.
[12] *Id*.
[13] Data Breach Notice, Exhibit B.
[14] *Id.*
[15] *See Id.*
[16] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/6a11760a-5f54-4fa7-b222-f74eed5cf516.shtml

32. Defendant did not have adequate security protocols to prevent, detect, and stop the cybercriminals from executing the cyberattack on CCC's systems and accessing the voluminous PII of Plaintiff and the proposed Class Members which was stored therein in the Data Breach.

33. Further, CCC failed to adequately train its employees on reasonable cybersecurity protocols and failed to implement reasonable security measures, causing it to lose control over individuals' PII in the Data Breach.

34. Defendant's tortious conduct and breach of contractual obligations, as explained hereinafter, are evidenced by its failure to recognize the Data Breach until cybercriminals had already accessed the data, meaning CCC had no effective means to detect and prevent attempted data breaches.

35. As a result of CCC's Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their dates of birth and Social Security numbers. Accordingly, CCC's identity theft protection through Kroll is wholly insufficient to compensate Plaintiff and the Class Members for their damages caused by the Data Breach.

36. Indeed, as a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, including identity theft and fraudulent charges, being forced to expend significant time and effort to remediate the consequences of the breach, as well as anxiety and emotional distress.

C. Plaintiff's Experience

37. Plaintiff was a debtor of CCC whose medical debt was purchased by Defendant approximately three (3) years ago and then paid in full.

38. In connection with the purchase of the debt, CCC obtained Plaintiff's PII which it stored on its computer systems.

39. On or about June 12, 2023, Plaintiff received CCC's Data Breach Notice, informing her that her name, Social Security Number, medical provider, dates of service, patient account number, and patient account balance had been compromised in the Data Breach.

40. After receiving the Data Breach Notice, Plaintiff signed-up for CCC's identity theft protection with Kroll.

41. To her knowledge, Plaintiff has never been the victim of a prior data breach.

42. As a direct result of the Data Breach, Plaintiff has suffered injury and damages, including identity theft, fraudulent misuse of her PII, and fraudulent charges, including:

a. Fraudulent activity on her Virginia Retirement System (VRS) account, for which Plaintiff received notification that $134.00 had been withdrawn and the account closed, requiring Plaintiff to re-register the account, when no monies had been withdrawn; and,

b. dramatic increase in spam texts and telephone calls.

43. Given the above fraudulent use of Plaintiff's PII following the Data Breach, it is obvious that her PII unauthorizedly disclosed in the Data Breach is now in the possession of cybercriminals and/or on the Dark Web and being utilized for fraudulent and criminal purposes.

44. In addition to the above fraudulent charges, Plaintiff has spent time and effort attempting to remediate the harmful effects of the Data Breach, and fears for her personal financial security and uncertainty over the information compromised in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. 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.

45. Plaintiff was highly disturbed by the Data Breach's nature and the thought of cybercriminals accessing her highly sensitive PII and the harm caused by the Data Breach.

46. As a result of CCC's Data Breach, Plaintiff faces a lifetime risk of additional identity theft, as it includes sensitive information that cannot be changed, like her date of birth and Social Security number.

D. This Data Breach was Foreseeable by CCC.

47. Plaintiff's and the proposed Class Members' PII was provided to CCC with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendant put all Class Members at risk of identity theft, financial fraud, and other harms.

48. Defendant tortiously failed to take the necessary precautions required to safeguard and protect the PII of Plaintiff and the Class Members from unauthorized disclosure. Defendant's actions represent a flagrant disregard of Plaintiff's and the other Class Members' rights.

49. Plaintiff and Class members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing PII and the critical importance of providing adequate security for that information.

50. Cyber-attacks against institutions such as Defendant are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of customer data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in

spear-phishing campaigns."[17] In fact, "40% [of financial institutions] have been victimized by a ransomware attack."[18]

51. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent)."[19]

52. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including CCC. According to IBM's 2022 report, "[f]or 83% of companies, it's not if a data breach will happen, but when."[20]

53. Based on data from the Maine Attorney General, as of August 2022, "…at least 79 financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million."[21]

54. PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including

---

[17]Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en (last acc. Jun 8, 2023).

[18] *Id.,* pg. 15.

[19] *See* "Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises," Jan. 24, 2022, available at https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/ (last acc. Apr. 14, 2023).

[20] IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at https://www.ibm.com/reports/data-breach (last acc. Apr. 14, 2023).

[21] Carter Pape, "Breach data from Maine shows scope of bank, credit union exposures," American Banker, August 24, 2022, available at https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures

ransomware and fraudulent misuse, and sale on the Dark Web.

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

56. Given the nature of the Data Breach, it was foreseeable that the compromised PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. CCC Failed to Comply with FTC Guidelines

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

58. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. 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.[22]

59. 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.[23]

60. 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 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.

61. These FTC enforcement actions include actions against entities failing to safeguard PII such as Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

62. CCC failed to properly implement basic data security practices widely known throughout the industry. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customer PII constitutes an unfair act or practice prohibited

[22] *See* Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).
[23] *See id*.

by Section 5 of the FTC Act, 15 U.S.C. § 45.

63. Defendant was at all times fully aware of its obligations to protect the PII of those individuals against whom it was collecting debts. CCC was also aware of the significant repercussions that would result from its failure to do so.

F. CCC Fails to Comply with Industry Standards

64. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards.

65. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[24]

66. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra,* such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.

[24] *See* Rapid7, "CIS Top 18 Critical Security Controls Solutions," available at https://www.rapid7.com/solutions/compliance/critical-controls/ (last acc. June 8, 2023).

- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.
- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.[25]

67. Further still, the Cybersecurity & Infrastructure Security Agency makes specific recommendations to organizations to guard against cybersecurity attacks, including (1) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (2) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (3) "[e]nsur[ing] that the organization is prepared to respond if an

[25] Federal Trade Commission, "Understanding The NIST Cybersecurity Framework," https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework (last acc. Apr. 14, 2023).

intrusion occurs," and other steps.[26]

68. Upon information and belief, CCC failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, as well as failing to comply with other industry standards for protecting Plaintiff's and the proposed Class Members' PII, resulting in the Data Breach.

G. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

69. Plaintiff and members of the proposed Class have suffered injury and damages from the misuse of their PII that can be directly traced to CCC, that has occurred, is ongoing, and/or imminently will occur.

70. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiff's and the proposed Class Members' PII, which is now being used for fraudulent purposes and has been sold for such purposes, causing widespread injury and damages.

71. The ramifications of CCC's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

72. Because CCC failed to prevent the Data Breach, Plaintiff and the proposed Class

[26] Cybersecurity & Infrastructure Security Agency, "Shields Up: Guidance for Organizations," available at https://www.cisa.gov/shields-guidance-organizations (last acc. June 8, 2023).

Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiff and the Class Members have suffered, will imminently suffer, or are at an increased risk of suffering:

a. Fraudulent misuse of PII;

b. The loss of the opportunity to control how PII is used;

c. The diminution in value of their PII;

d. The compromise and continuing publication of their PII;

e. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

f. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

g. Delay in receipt of tax refund monies;

h. Increase in spam texts and telephone calls;

i. Unauthorized use of stolen PII; and

j. The continued risk to their PII, which remains in the possession of CCC and is subject to further breaches so long as CCC fails to undertake the appropriate measures to protect the PII in its possession.

73. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

74. There are myriad dangers which affect victims of identity theft, including:

cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.[27]

75. The FTC recommends that identity theft victims take time and effort intensive or costly steps to protect their personal and financial information after a data breach, including contacting the company where the fraud occurred and asking them to close or freeze accounts and changing login information; contacting one of the credit bureaus to place a fraud alert on credit files (consider an extended fraud alert that lasts for 7 years if someone steals their identity); reviewing their credit reports; seeking a credit freeze; correcting their credit reports; and other steps such as contacting law enforcement and reporting the identity theft to the FTC.[28]

76. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud—just as occurred here—phone or utilities fraud, and bank/finance fraud.

---

[27] *See* Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score (last acc. Feb. 27, 2023).

[28] *See* Federal Trade Commission, available at https://www.identitytheft.gov/Steps (last acc. June 8, 2023).

77. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

78. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive other services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

79. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. 35% reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. 54% percent reported feelings of being violated. [29]

80. What's more, theft of PII is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII/PHI is a valuable property right.[30]

---

[29] Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ citing Identity Theft Resource Center, "2021 Consumer Aftermath Report," May 26, 2021 available at https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/ (last acc. Feb. 27, 2023).

[30] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private information, which companies obtain at little cost,

81. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that PII has considerable market value.

82. It must also be noted there may be a substantial time lag–measured in years–between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

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

84. Where the most PII belonging to Plaintiff and Class Members was accessible from CCC's network, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and the Class Members must vigilantly monitor their financial accounts for many years to come.

85. While credit card information can sell for as little as $1-$2 on the black market, other more sensitive information can sell for as much as $363, according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams, posing as medical personnel through the use of otherwise sacrosanct information. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

---

has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

86. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.[31]

87. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[32] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

88. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[33]

89. This data, as one would expect, demands a much higher price on the black market.

---

[31] *See* U.S. Social Security Administration, "Identity Theft and Your Social Security Number," Publication No. 05-10064, July 2021, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last acc. Feb. 25, 2023)

[32] *See id.*

[33] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited September 1, 2021).

Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[34] Medical information is especially valuable to identity thieves. The asking price on the Dark Web for medical data is $50 per person and up.[35]

102. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the criminal fraudulent activity, fraudulent charges, and attendant costs, lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

103. CCC knew or should have known of these harms which would be caused by the Data Breach they permitted to occur, and strengthened its data systems accordingly.

CLASS ALLEGATIONS

114. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

115. Plaintiff brings this nationwide class action individually and on behalf of all other persons similarly situated pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

116. Plaintiff proposes the following Class definition, subject to amendment based on information obtained through discovery:

---

[34] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited June 13, 2023).

[35] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LogDog (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/ (last accessed June 13, 2023).

All persons whose PII was compromised as a result of the Data Breach experienced by Defendant beginning on March 2, 2023 as announced by CCC, including all persons who received the Data Breach Notice.

117. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

118. Plaintiff reserves the right to amend the definition of the Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

119. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

120. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

121. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the PII of approximately 286,699 individuals was compromised in the Data Breach. Such information is readily ascertainable from Defendant's records.

122. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class

Members. These common questions of law and fact include, without limitation:

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

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

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

e. Whether computer hackers obtained Plaintiff's and Class Members' PII in the Data Breach;

f. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

g. Whether CCC failed to adequately respond to the Data Breach, including failing to timely notify the Plaintiff and the Class Members;

h. Whether Defendant's failures amounted to negligence;

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

j. Whether Defendant was unjustly enriched;

k. Whether Defendant's acts violated the law, and;

l. Whether Plaintiff and the Class Members are entitled to damages including

compensatory and punitive damages, and/or injunctive relief.

123. **Typicality, Fed. R. Civ. P. 23(a)(3):** 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 same violations of law. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

124. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

125. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data—PII—was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

126. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. 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 Defendant 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 Defendant to all Class Members, in terms of money damages due and in 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 Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with 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 CCC's partners' customers or its debtors, 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 Defendant's records, such that direct notice to the Class Members would be appropriate.

127. In addition, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

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

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

130. Defendant collected and stored the PII of Plaintiff and the proposed Class Members.

131. Defendant had full knowledge of the sensitivity of the PII to which it was entrusted, and the types of harm that Plaintiff and the Class Members could and would suffer if the PII was wrongfully disclosed to unauthorized persons. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information.

132. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their data in Defendant's possession.

133. By collecting and storing this data in its computer systems, Defendant had a duty of care to use reasonable means to secure and safeguard it, to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect if that PII was exposed to the internet and to give prompt notice to those affected in the case of a data breach.

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

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

136. Defendant breached its duties, and was negligent, by acts of omission or commission, by failing to use reasonable measures to protect the Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

b. Failing to adequately train employees on proper cybersecurity protocols;

c. Failing to adequately monitor the security of its networks and systems;

d. Failure to periodically ensure that its network system had plans in place to maintain reasonable data security safeguards;

e. Allowing unauthorized access to Plaintiff's and Class Members' PII;

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

137. It was foreseeable that Defendant's failure to use reasonable measures to protect Plaintiff's and Class Members' PII would result in injury to Plaintiff and Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyber-attacks and data breaches in the industry.

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

139. As a direct and proximate result of Defendant's negligence set forth in the preceding paragraphs, Plaintiff and Class Members have suffered injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to compensatory, actual, and punitive damages as a result of the Data Breach.

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

COUNT II
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

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

142. Plaintiff and proposed Class Members conferred benefits upon Defendant in the form of monies received by CCC for debt collection services, and in the form of valuable PII entrusted to Defendant.

143. Defendant appreciated or knew of these benefits that it received. And under principles of equity and good conscience, this court should not allow Defendant to retain the full value of these benefits—specifically, the monies, and PII of Plaintiff and members of the Class.

144. After all, Defendant failed to adequately protect Plaintiff's and Class Members' PII. And if such inadequacies were known, then Plaintiff and the members of the Class would never have conferred payment to Defendant, nor disclosed their PII.

145. As a direct and proximate result of Defendant's unjust enrichment set forth in the preceding paragraphs, Plaintiff and Class Members have suffered injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to damages as a result of the Data Breach.

146. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and members of the Class—all funds that were unlawfully or inequitably gained despite Defendant's misconduct and the resulting Data Breach.

COUNT III
INVASION OF PRIVACY—INTRUSION UPON SECLUSION
(On Behalf of Plaintiff and the Class)

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

148. Plaintiff and the Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

149. Defendant owed a duty to Plaintiff and the Class Members, to keep their PII confidential.

150. Defendant failed to protect said PII and exposed the PII of Plaintiff and the Class Members to unauthorized persons which is now publicly available, including on the dark web, and being fraudulently misused.

151. Defendant allowed unauthorized third parties access to and examination of the PII of Plaintiff and the Class Members, by way of Defendant's failure to protect the PII.

152. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and the Class Members is highly offensive to a reasonable person.

153. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff's and the Class Members' PII was disclosed to Defendant in connection with CCC's debt collection efforts, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

154. The Data Breach constitutes an intentional or reckless interference by Defendant with Plaintiff's and the Class Members' interests in solitude or seclusion, either as to their persons

or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

155. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its data security practices were inadequate and insufficient.

156. Defendant acted with reckless disregard for Plaintiff's and Class Members' privacy when they allowed improper access to its systems containing Plaintiff's and Class Members' PII.

157. Defendant was aware of the potential of a data breach and failed to adequately safeguard its systems and implement appropriate policies to prevent the unauthorized release of Plaintiff's and Class Members' PII.

158. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Class Members.

159. As a direct and proximate result of the Defendant's invasion of privacy, the PII of Plaintiff and the Class Members was disclosed to third parties without authorization, causing Plaintiff and the Class Members to suffer injury and damages as set forth herein, including monetary damages, fraudulent misuse of their PII and fraudulent charges; loss of the opportunity to control how their PII is used; diminution in value of their PII; compromise and continuing publication of their PII; and are entitled to damages.

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

161. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and the Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, JORDAN HAMILTON, on behalf of herself, and all others similarly situated, prays for judgment as follows:

A. Trial by jury pursuant to Fed. R. Civ. Proc. 38(b) on all claims so triable;

B. An Order certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

C. Awarding Plaintiff and the Class damages that include applicable compensatory, actual, exemplary, and statutory damages, and punitive damages, as allowed by law;

D. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

E. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

F. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

G. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the transmitted PII;

H. Awarding attorneys' fees and costs, as allowed by law;

I. Awarding prejudgment and post-judgment interest, as provided by law;

J. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and,

K. Any and all such relief to which Plaintiff and the Class are entitled.

Dated: June 15, 2023

Respectfully submitted,

/s/ *Devon J. Munro*
Devon Munro (VSB # 47833)
MUNRO BYRD, P.C.
120 Day Avenue SW, First Floor
Roanoke, Virginia 24016
Ph.: 540-283-9343
Fax: 540-328-9290
dmunro@trialsva.com

Lynn A. Toops*
Mary Kate Dugan*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
(317) 636-6481
ltoops@cohenandmalad.com
mdugan@cohenandmalad.com

J. Gerard Stranch, IV *
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
(615) 254-8801
(615) 255-5419 (facsimile)
gstranch@stranchlaw.com
amize@stranchlaw.com

Samuel J. Strauss*
TURKE & STRAUSS, LLP
613 Williamson St., Suite 201
Madison, Wisconsin 53703
(608) 237-1775

(608) 509-4423 (facsimile)
sam@turkestrauss.com

*Motion for *Pro Hac Vice* Admission forthcoming

Counsel for Plaintiff and the Proposed Class