UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA

NIVEDITA SHARMA, individually and on behalf of all others similarly situated, Plaintiff, v. ACCUTECH SYSTEMS CORPORATION, Defendant.	No. _____

CLASS ACTION COMPLAINT

Plaintiff Nivedita Sharma ("Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Accutech Systems Corporation ("Accutech" or "Defendant"), by and through her attorneys, and alleges, based upon personal knowledge as to her own actions and her counsels' investigation, and based upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Accutech is a technology company that provides personalized technology services to more than 200 banks and wealth management institutions across the United States.[1]

2. As an accounting and wealth management technology company, Accutech collects, maintains, and stores its clients' customers' highly sensitive personal and financial information including, but not limited to: full names, Social Security numbers, dates of birth, financial account

[1] *About Accutech*, Accutech Systems, https://www.trustasc.com/about/ (last accessed Mar. 14, 2022).

information, payment card numbers, and account access information ("personally identifying information" or "PII").[2]

3. Although Accutech is a sophisticated entity that provides critical information technology services to equally sophisticated corporate clients, Accutech itself failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive personal and financial information of approximately 40,000 individuals, including the Plaintiff and the Class. As a direct, proximate, and foreseeable result of Accutech's failure to implement reasonable security protections sufficient to prevent an eminently avoidable cyberattack, unauthorized actors compromised Accutech's network and accessed tens of thousands of client files containing highly-sensitive PII.[3]

4. Specifically, on August 16, 2021, Accutech's sensitive customer data was compromised when cybercriminals were able to breach Accutech's network and access files containing approximately 39,518 individual's PII (the "Data Breach").[4]

5. Despite the fact that many of the categories of PII exposed in the Data Breach, such as Social Security numbers and dates of birth, cannot be changed, Accutech failed to provide notice of the Breach to Plaintiff and other individuals affected by the Data Breach ("the Class") until on or around February 7, 2022—more than one month after Accutech supposedly detected the Data

[2] *Accutech Systems Corporation, February 4, 2022*, New Hampshire Department of Justice Office of the Attorney General, https://www.doj.nh.gov/consumer/security-breaches/documents/accutech-systems-20220204.pdf (last accessed Mar. 14, 2022); *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/ec58a339-1914-466e-8db5-6d995b70cdc4.shtml (last accessed Mar. 14, 2022); *Data Breach Notification Report*, Commonwealth of Massachusetts, Office of Consumer Affairs and Business Regulation, https://www.mass.gov/doc/data-breach-report-2022/download (last accessed Mar. 14, 2022).

[3] *Id.* (noting that Accutech informed multiple Attorney General's Offices that a data breach occurred on August 16, 2021) (last accessed Mar. 14, 2022).

[4] *Id.*

Breach, and more than **six months** after unauthorized individuals accessed Plaintiff's and Class members' highly sensitive PII stored on Accutech's systems.

6. Accutech's failure to promptly notify Plaintiff and Class members that their PII was exfiltrated due to Acccutech's security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse and/or disseminate that PII before Plaintiff and the Class could take affirmative steps to protect their sensitive information. As a result, Plaintiff and the Class will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

7. Accutech failed to take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to current and former clients and their customers the material fact that it lacked appropriate data systems and security practices to secure PII and financial information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to Accutech's failures, Plaintiff and approximately 40,000 individuals nationwide suffered substantial harm and injury.

8. As a result of Accutech's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third-parties for the express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of the current and former customers of Accutech's clients. Plaintiff and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors.

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

10. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief from Accutech's failure to reasonably safeguard Plaintiff's and Class members' PII; its failure to reasonably provide timely notification that Plaintiff's and Class members' PII had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their PII.

II. PARTIES

Plaintiff Sharma

11. Plaintiff Nivedita Sharma ("Plaintiff") is a resident and citizen of Colorado, residing in Englewood, Colorado.

12. Plaintiff received Accutech's *Notice of Data Breach* (the "Notice") after February 7, 2022.

13. On information and belief, Plaintiff was at some point a user or accountholder at Centier Bank, a privately owned bank headquartered in Merrillville, Indiana. According to the Notice Plaintiff received, Accutech came to possess Plaintiff's PII because Accutech provides certain "accounting software services" to Centier Bank, and Plaintiff was "listed as a user or account holder for an account at Centier Bank."

14. Plaintiff provided her PII to Centier with the expectation that Centier and its agents, including Accutech, would exercise reasonable care to protect and maintain the confidentiality of her PII and other confidential information by safeguarding it from compromise, disclosure, and misuse by unauthorized actors, except to the extent necessary to provide agreed-upon financial services, and would be timely and forthright relating to any data security incidents involving his PII.

15. In the Notice that Plaintiff received after February 7, 2022, Accutech informed her that her name and Social Security number may have been both "accessed and acquired from [Accutech's] network by an unauthorized party." Accutech also advised her to "place an initial one (1) year fraud alert on [her] credit files" and review a recent credit report in order to guard against the concrete risks the Data Breach imposed upon her. Further, although Accutech asserted in the Notice that it has "no evidence" Plaintiff's PII was "misused," Accutech impliedly concedes her PII was exfiltrated because it informed Plaintiff "[w]e have also taken steps to . . . regain possession of the data and ensure its safekeeping."

16. The Data Breach already has required Plaintiff to expend significant time and effort to protect herself and her family from its potential adverse consequences, including but not limited

to investigating whether hackers have further attempted to misuse her PII, and potential means by which to protect herself from identity theft, such as by placing fraud alerts on her credit accounts at major credit bureaus, reviewing her credit reports, changing the passwords to her various accounts and monitoring associated bank and credit accounts. Since she received the Data Breach notification, Plaintiff believes she has spent at least 2-3 hours per week taking the aforesaid mitigation measures.

17. In addition, in the wake of the Data Breach, Plaintiff received an alert from Experian advising her that her email password had been found on the Dark Web.

18. Further, Plaintiff has received an uptick in spam text messages since the Data Breach. Plaintiff receives at least 5 spam text messages per day, all of which appear to be placed with the intent to commit identity theft by way of reverse social engineering.

19. As a direct, proximate and foreseeable result of the Data Breach, as well as Defendant's failure to prevent against and timely notify Plaintiff of the same, Plaintiff has suffered concrete injuries and damages, including out-of-pocket costs incurred in mitigating the immediate effects of the Data Breach and the heightened risk of fraud and identity theft to which the Breach exposed her.

Defendant Accutech

20. Defendant Accutech Systems Corporation is corporation organized under the laws of the State of Indiana, with its principal place of business at 115 South Walnut Street, Muncie, Indiana 47305.

III. JURISDICTION AND VENUE

21. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and

Defendant is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

22. This Court has personal jurisdiction over Defendant because it is authorized to and regularly conducts business in Indiana, and is headquartered in Muncie, Indiana.

23. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Accutech Systems Corporation - Background

24. Accutech provides technical, accounting, and financial services to more than 200 banks and wealth management institutions throughout the United States.[5] Accutech represents that it provides its clients with data and technological services that include anomalous data activity detection, information technology specialists, and data disaster services.[6]

25. As part of their financial business operations, Accutech collects, maintains, and stores the highly sensitive PII and financial information provided by the customers of its current and former clients' customers, including but not limited to: full names, Social Security numbers, dates of birth, financial account numbers, payment card information, and account access information.

[5] *About Accutech*, Accutech Systems, https://www.trustasc.com/about/ (last accessed Mar. 14, 2022).
[6] *See, e.g.*, *Solutions*, Accutech Systems, https://www.trustasc.com/solutions/ (last accessed Mar. 15, 2022); *Insights*, Accutech Systems, https://www.trustasc.com/insights/ (last accessed Mar. 15, 2022); *Business Process Outsourcing*, Accutech Systems, https://www.trustasc.com/business-process-outsourcing/ (last accessed Mar. 15, 2022).

26. On information and belief, at the time of the Data Breach, and despite its claims that it is experienced in detecting anomalous data activity detection and providing "data disaster services," Accutech had failed to implement necessary data security safeguards, which resulted in unauthorized third parties accessing the PII of nearly 40,000 current and former customers of Accutech's clients.

27. Current and former customers of Acccutech's clients, such as Plaintiff and the Class, allowed their PII to be made available to Accutech with the reasonable expectation that Accutech would comply with its obligation to keep their sensitive and personal information, including their PII, confidential and secure from illegal and unauthorized access, and that Accutech would provide them with prompt and accurate notice of any unauthorized access to their PII.

28. Unfortunately for Plaintiff and Class members, Accutech failed to carry out its duty to safeguard sensitive PII and provide adequate data security, thus failing to protect Plaintiff and Class members from the exfiltration of their PII during the Data Breach.

B. The Data Breach

29. Accutech disclosed in a Notice sent on or about February 7, 2022, to Plaintiff and other affected individuals that it was affected by a cybersecurity incident—the Data Breach—and that Plaintiff's and other individual's sensitive PII had been compromised. Further, acknowledges that the unauthorized actors were able to exfiltrate Plaintiff's and Class members' PII and financial information, stating that it is attempting to "regain possession" of the data..

30. According to the Notice, "unauthorized access to [Accutech's] network occurred on August 16, 2021."

31. Accutech admits in the Notice that it did not detect the Data Breach until on or about December 27, 2021, more than four months after the unauthorized individuals first gained unfettered access to Accutech's data systems.

32. Accutech asserts that upon discovering the Data Breach, it began an investigation and determined on or about December 27, 2021, that Accutech's clients' current and former customers' "name and Social security number may have been accessed and acquired from [Accutech's] network by an unauthorized party."

33. Accutech further confirmed that on or about January 11, 2022, it began notifying Accutech's financial institution clients about the Data Breach. However, Accutech delayed in sending individualized notice to affected customers of Accutech's financial institution clients until on or after February 7, 2022.

34. Accutech has not yet acknowledged the full extent of PII that was improperly accessed by unauthorized third parties in the Data Breach. For example, the Notice sent to Plaintiff advises her that the unauthorized actors gained access to her full name and Social Security numbers. However, Accutech admitted in a filing with the Maine Attorney General that the unauthorized actors also gained access to Accutech's clients' current and former customers' financial account numbers and credit/debit card numbers (in combination with the security code, access code, password, or PIN for the account).[7]

35. Additionally, Accutech has not acknowledged the length of time that unauthorized individuals had access to Accutech's network, stating only that Accutech's Data Breach occurred on August 16, 2021, and that the Data Breach was detected on December 27, 2021. However,

[7] *See Accutech Systems Corporation Data Breach Notification*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/ec58a339-1914-466e-8db5-6d995b70cdc4.shtml.

based on the type of PII accessed and exfiltrated, the unauthorized individuals likely had access to Accutech's network for a significant period of time prior to and/or after August 16, 2021.

36. During the time that the unauthorized individuals had unrestricted access to Accutech's network, they were able to access and acquire personal, sensitive, and protected PII belonging to approximately 40,000 current and former customers of Accutech's clients.

C. Accutech's Many Failures Both Prior to and Following the Breach

37. Accutech could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and network files containing PII.

38. In the Notice, Accutech acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to virtually every aspect of Accutech's operations as a technology firm providing services to hundreds of wealth management and financial institution clients. Accutech acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

39. Despite such representations, and its purported expertise in detecting anomalous data activity and providing "data disaster services," Accutech failed to detect that its own data system was compromised until December 27, 2021.

40. Further, despite detecting the Data Breach on December 27, 2021, Accutech waited until January 11, 2022, to begin notifying its financial institution clients of the Data Breach, and did not provide direct notice to the individuals whose PII and financial information was accessed in the Data breach until on or after February 7, 2022—almost six months after the Data Breach occurred, and almost two months after it first detected the Data Breach.

41. Moreover, when Accutech finally acknowledged that it had experienced a breach, it failed to fully inform affected individuals of the length of time that the unauthorized actors had access to their PII, or even the full extent of the PII that was accessed during the Data Breach.

42. Accutech's failure to properly safeguard Plaintiff's and Class members' PII allowed the unauthorized actors to access this highly sensitive PII and financial information, and Accutech's failure to timely notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

43. The Data Breach also highlights the inadequacies inherent in Accutech's network monitoring procedures. If Accutech had properly monitored its cyber security systems, it would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from exfiltrating PII and financial information.

44. Accutech's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

45. First, Accutech filed to timely notify affected individuals, including Plaintiff and Class members, that Accutech had allowed their highly-sensitive PII to be accessed by unauthorized third parties.

46. Second, Accutech has made no effort to protect Plaintiff and the Class from the long-term consequences of Accutech's acts and omissions. Although the Notice offered victims a complimentary one year membership to Experian Identity Works, Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long beyond one year. As a result, Plaintiff and the Class will remain at a heightened and unreasonable

risk of identity theft for the remainder of their lives, a risk that a single year of credit monitoring cannot remedy.

47. In short, Accutech's myriad failures, including to timely detect the Data Breach and to notify Plaintiff and Class member with reasonable timeliness that their personal and financial information had been exfiltrated due to Accutech's security failures, allowed unauthorized individuals to access and misappropriate Plaintiff's and Class members' PII for months before Accutech finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

48. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

49. In 2018, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a 126% increase in exposed data.[8]

50. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[9]

51. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being exposed exceeding

[8] *2018 End of Year Data Breach Report*, Identity Theft Resource Center, available at https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf (last accessed Mar. 14, 2022).
[9] *2019 End of Year Data Breach Report*, Identity Theft Resource Center, available at https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Mar. 14, 2022).

100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[10]

52. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[11]

53. In fact, Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach incidents.[12] Conditions have only worsened since: Statista estimates that "[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]" and that "[i]n the first half of 2020, there were 540 reported data breaches."[13]

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

55. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers

---

[10] *Id.*
[11] *Id.*
[12] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed (last accessed Mar. 14, 2022).
[13] *Id.*

have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

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

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

58. Further, consumers' PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, available at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Mar. 17, 2022).

value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[15]

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[16]

60. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

61. 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."[17]

---

[15] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, available at https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed Mar. 17, 2022).

[16] Social Security Administration, *Identity Theft and Your Social Security Number*, available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Mar. 17, 2022).

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed Mar. 17, 2022).

62. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[18]

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

64. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[19] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

65. To date, Accutech has offered its consumers *only one year* of identity monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the threats they face for years to come, particularly in light of the PII at issue here.

66. Despite the prevalence of public announcements of data breach and data security compromises, its own expertise in the information technology sector, and its own acknowledgment

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), available at http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar. 17, 2022).
[19] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, available at https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed Mar. 17, 2022).

of its duties to keep PII private and secure, Accutech failed to take appropriate steps to protect the PII of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Accutech's failure to implement or maintain adequate data security measures for its client's current and former customers.

E. Accutech had a Duty and Obligation to Protect PII

67. Accutech has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. Accutech's obligations are derived from: 1) government regulations and state laws, and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided, and Accutech obtained, their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[20] 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."[21]

[20] 17 C.F.R. § 248.201 (2013).
[21] *Id.*

69. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[22]

70. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[23] The guidelines note businesses should protect the personal information that 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 security problems.[24] 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.[25] Accutech clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, and the amount of data exfiltrated.

71. Here, at all relevant times, Accutech was fully aware of its obligation to protect the PII of current and former customers of its clients, including Plaintiff and the Class, because it is a sophisticated and technologically savvy financial business entity that relies extensively on technology systems and networks, and routinely maintains and transmits customers' PII and financial information in order to operate its business.

---

[22] *Start With Security*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf. (last accessed Mar. 14, 2022).
[23] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (Jan. 23, 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business. (last accessed Mar. 14, 2022).
[24] *Id.*
[25] *Id.*

72. Accutech had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the PII and financial information from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Accutech and Plaintiff and Class members. Accutech alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' PII.

73. Accutech's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential client data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

74. Further, Accutech had a duty to promptly notify Plaintiff and the Class that their PII was accessed by unauthorized persons.

F. Accutech Violated FTC and Industry Standard Data Protection Protocols

75. The FTC rules, regulations, and guidelines obligate business to protect PII, from unauthorized access or disclosure by unauthorized persons.

76. Unfortunately, Accutech failed to comply with FTC rules, regulations and guidelines, and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Accutech failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of clients' current and former customers' PII;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its clients' current and former customers' PII;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its clients' current and former customers' PII.

77. Had Accutech implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Accutech could have prevented or detected the Data Breach prior to the hackers accessing Accutech's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former customer of Accutech's clients would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. Accutech's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

78. Accutech purports to care about data security and safeguarding clients' PII, and represents that it will keep secure and confidential the PII belonging to its clients' current and former customers.

79. Plaintiff's and Class members' PII and financial information was provided to Accutech in reliance on its promises and self-imposed obligations to keep PII and financial information confidential, and to secure the PII and financial information from unauthorized access by malevolent actors. It failed to do so.

80. The length of the Data Breach also demonstrates that Accutech failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors to periodically test its network, servers, systems and workstations.

81. Had Accutech undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Accutech would have detected the Data Breach prior to the hackers extracting data from Accutech's networks, and current and former customers of Accutech's clients would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

82. Indeed, following the Data Breach, Accutech effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiff and others, Accutech acknowledged that the Data Breach required it to implement multiple remedial measures to protect its clients' former and current customers from "potential misuse of [their] information."

H. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

83. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[26]

84. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC

[26] Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*, CNET (Oct. 1, 2015), available at: http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/. (last accessed Mar. 14, 2022).

notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[27]

85. The ramifications of Accutech's failure to properly secure PII, including Plaintiff's and Class members' PII, are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission to commit fraud or other crimes.

86. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

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

88. Accordingly, Accutech's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.[28] Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach."[29] Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers

[27] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed Mar. 14, 2022).
[28] *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), available at http://www.iii.org/insuranceindustryblog/?p=267 (last accessed Mar. 17, 2022).
[29] Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), available at http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php (last accessed Mar. 17, 2022).

at a substantial risk of fraud."[30] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class members' PII will do so at a later date or re-sell it.

89. In response to the Data Breach, Accutech offered to provide certain individuals whose PII was exposed in the Data Breach with one year of credit monitoring. However, one year of complimentary credit monitoring is a time frame much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by Accutech's' failures.

90. Moreover, the credit monitoring offered by Accutech is inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive PII.

91. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and

[30] THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, available at https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed Mar. 17, 2022).

annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Accutech's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

92. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being accessed by cybercriminals, risks that will not abate within a mere year: the unauthorized access of Plaintiff's and Class members' PII, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Accutech offered victims of the Breach. The one year of credit monitoring that Accutech offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class members have suffered and will continue to suffer as a result of the Data Breach.

93. As a direct and proximate result of Accutech's acts and omissions in failing to protect and secure PII and financial information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

94. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both herself and similarly situated individuals whose PII was accessed in the Data Breach.

95. Accutech is aware of the ongoing harm that the Data Breach has and will continue to impose on current and former customers of Accutech's clients, as the notices that it posted and sent to Plaintiff and Class members regarding the Data Breach advise the victims to review their

"financial account statements and credit reports for fraudulent or irrelevant activity on a regular basis."

V. CLASS ALLEGATIONS

96. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose PII was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

97. In the alternative, Plaintiff brings this action on behalf of herself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Colorado whose PII was accessed in the Data Breach (the "Colorado Subclass").

Excluded from the Colorado Subclass are Defendants, its executives and officers, and the Judge(s) assigned to this case.

98. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Accutech and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that more than tens of thousands individuals comprise the Class and were affected by the Data Breach. Indeed, Accutech admitted that the Data Breach affected more than 39,500

individuals in its notification to the Maine Attorney General's Office.[31] The members of the Class will be identifiable through information and records in Accutech's possession, custody, and control.

99. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Accutech's data security and retention policies were unreasonable;

b. Whether Accutech failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Accutech owed a duty to Plaintiff and Class members to safeguard their PII;

d. Whether Accutech breached any legal duties in connection with the Data Breach;

e. Whether Accutech's conduct was intentional, reckless, willful or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether Accutech breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Accutech's conduct; and

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

[31] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/ec58a339-1914-466e-8db5-6d995b70cdc4.shtml (last accessed Mar. 14, 2022)

100. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their PII compromised in the Data Breach. Plaintiff and the members of the Class sustained damages as a result of Accutech's uniform wrongful conduct.

101. Adequacy: Plaintiff is an adequate representative because her interests do not materially or irreconcilably conflict with the interests of the Class she seeks to represent, she has retained counsel competent and highly experienced in complex class action litigation, and intends to prosecute this action vigorously. Plaintiff and her counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor her counsel have any interests that are antagonistic to the interests of other members of the Class.

102. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Accutech's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Accutech's records and databases.

103. Accutech has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

VI. CLASS ALLEGATIONS

COUNT I –- Negligence
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

104. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

105. This count is brought on behalf of all Class members.

106. Accutech owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Accutech collected.

107. Accutech owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Accutech collected.

108. Accutech owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

109. Accutech owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

110. Accutech solicited, gathered, and stored the PII belonging to Plaintiff and the Class.

111. Accutech knew or should have known it inadequately safeguarded this information.

112. Accutech knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and the Class, and Accutech was therefore charged with a duty to adequately protect this critically sensitive information.

113. Accutech had a special relationship with Plaintiff and the Class. Plaintiff's and Class members' highly sensitive PII and financial information was entrusted to Accutech on the understanding that adequate security precautions would be taken to protect the PII and financial

information. Moreover, only Accutech had the ability to protect its systems and the PII stored on them from attack.

114. Accutech's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. Accutech's misconduct included failing to: (1) secure its systems, servers and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

115. Accutech breached its duties to Plaintiff and the Class by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiff and the Class.

116. Accutech breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

117. Accutech breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

118. The law further imposes an affirmative duty on Accutech to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

119. Accutech breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their PII had been improperly acquired or accessed.

120. Accutech breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until February 7, 2022.

121. As a direct and proximate result of Accutech's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

122. As a direct and proximate result of Accutech's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II –- Negligence *Per Se*
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

123. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Accutech, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Accutech's duty.

124. The Indiana Disclosure of Security Breach Act ("IDSBA") requires that entities in possession of PII belonging to Indiana residents that was or may have been accessed by unauthorized persons disclose the data breach without unreasonable delay. *See* In. Stat. § 24-4.9-1, *et seq.*

125. The Colorado Consumer Protection Act ("CCPA") requires that entities in possession of PII belonging to Colorado residents to: 1) protect PII from unauthorized access and disclosure, and 2) maintain reasonable security practices. *See* C.R.S. § 6-1-713.5. Further, the CCPA obligates entities in possession of PII to provide notice of the data breach within 30 days after discovery. *See* C.R.S. § 6-1-716.

126. In addition to the FTC rules and regulations, the IDSBA, and CCPA, other states and jurisdictions where victims of the Data Breach are located require that Accutech protect PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

127. Accutech violated the IDSBA, the CCPA and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards; and by unduly delaying reasonable notice of the actual breach. Accutech's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiff's and Class members' sensitive PII.

128. Accutech's violations of the IDSBA, the CCPA, Section 5 of the FTC Act and other applicable statutes, rules, and regulations constitutes negligence *per se*.

129. Plaintiff and the Class are within the category of persons the IDSBA, the CCPA and the FTC Act were intended to protect.

130. The harm that occurred as a result of the Data Breach described herein is the type of harm the IDSBA, the CCPA and FTC Act were intended to guard against.

131. As a direct and proximate result of Accutech's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Accutech's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III –- Breach of Implied Contract
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

132. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

133. This count is brought on behalf of all Class members.

134. Plaintiff and the Class provided Accutech with their PII and financial information.

135. By providing their PII, and upon Accutech's acceptance of such information, Plaintiff and the Class, on one hand, and Accutech, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

136. The implied contracts between Accutech and Plaintiff and Class members obligated Accutech to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Accutech expressly adopted and assented to these terms in its public statements, representations and promises as described above.

137. The implied contracts for data security also obligated Accutech to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII.

138. Accutech breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' PII; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

139. As a direct and proximate result of Accutech's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII in Accutech's possession, and are entitled to damages in an amount to be proven at trial.

COUNT IV –- Bailment
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

140. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

141. This count is brought on behalf of all Class members.

142. Plaintiff's and Class members' PII was provided to Accutech.

143. In delivering their PII, Plaintiff and Class members intended and understood that their PII would be adequately safeguarded and protected.

144. Accutech accepted Plaintiff's and Class members' PII.

145. By accepting possession of Plaintiff's and Class members' PII, Accutech understood that Plaintiff and the Class expected their PII to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

146. During the bailment (or deposit), Accutech owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their PII.

147. Accutech breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII.

148. Accutech further breached its duty to safeguard Plaintiff's and Class members' PII by failing to timely notify them that their PII had been compromised as a result of the Data Breach.

149. Accutech failed to return, purge or delete the PII belonging to Plaintiff and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

150. As a direct and proximate result of Accutech's breach of its duties, Plaintiff and the Class suffered consequential damages that were reasonably foreseeable to Accutech, including but not limited to the damages set forth herein.

151. As a direct and proximate result of Accutech's breach of its duty, Plaintiff's and Class members PII that was entrusted to Accutech during the bailment (or deposit) was damaged and its value diminished.

COUNT V –- Violation of the Indiana Deceptive Consumer Sales Act
Ind. Stat. § 24-5-0.5-1, *et seq.*
(By Plaintiff on behalf of the Class)

152. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

153. This count is brought on behalf of the Class.

154. The Indiana Deceptive Consumer Sales Act ("IDSCA"), Ind. Stat. § 24-5-0.5-1, *et seq.*, prohibits "[a] supplier [from] commit[ting] an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. . . ." Ind. Stat. § 24-5-0.5-3.

155. Accutech is a "supplier" as defined by Ind. Stat. § 24-5-0.5-2(a)(3).

156. Deceptive and unfair acts, practices, and omissions prohibited by the IDSCA include, but are not limited to:

a. Representing that the subject of a transaction has the performance characteristics, uses, or benefits which the supplier knows or should know that the subject of the transaction does not have;

b. Representing that the subject of a transaction is of a particular standard, quality, or grade that the supplier knows or should know that the subject of the transaction does not have; and

c. Advertising services with the intent not to sell them as advertised.

157. Accutech's deceptive acts, omissions, and conduct include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

158. Accutech had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' PII. This exclusive knowledge includes, but is not limited to, information that Accutech received through internal and other non-public audits and reviews that concluded that Accutech's security policies were substandard and deficient, and that Plaintiff's and Class members' PII and other Accutech data was vulnerable.

159. Accutech also had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

160. Accutech also had exclusive knowledge about the length of time that it maintained individual's PII after they stopped using Accutech's services.

161. Accutech failed to disclose, and actively concealed, the material information it had regarding Accutech's deficient security policies and practices, and regarding the security of the

sensitive PII and financial information. For example, even though Accutech has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' PII was vulnerable as a result, Accutech failed to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. Accutech also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former customers' PII and other records. Likewise, during the days and weeks following the Data Breach, Accutech failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

162. Accutech had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, it made affirmative statements that were inconsistent with the information it did not disclose, and because Accutech was in a fiduciary position by virtue of the fact that Accutech collected and maintained Plaintiff's and Class members' PII and financial information.

163. Accutech's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Accutech's data security and its ability to protect the confidentiality of current and former customers' PII.

164. Had Accutech disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Accutech would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Accutech received, maintained, and compiled Plaintiff's and Class members' PII without advising that Accutech's data security practices were insufficient to maintain the safety and confidentiality of their PII.

165. Accordingly, Plaintiff and Class members acted reasonably in relying on Accutech's misrepresentations and omissions, the truth of which they could not have discovered.

166. Accutech's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as the IDSBA, the CCPA and FTC Act.

167. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should have reasonably avoided.

168. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Accutech's deceptive acts and practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to Accutech as their clients, and with the understanding that Accutech would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Accutech and which is subject to further breaches so long as Accutech fails to undertake appropriate and adequate measures to protect data in its possession.

169. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Accutech from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VI — Violation of the Colorado Consumer Protection Act
C.R.S. § 6-1-105, *et seq.*
(By Plaintiff on behalf of the Colorado Subclass)

170. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

171. This count is brought on behalf of the Colorado Subclass.

172. The Colorado Consumer Protection Act ("CCPA"), C.R.S. § 6-1-105, *et seq.*, prohibits "[a] person [from engaging] in a deceptive trade practice . . . ." C.R.S. § 6-1-105(1).

173. Accutech is a "person" as defined by C.R.S. § 6-1-102(6).

174. Defendant engaged in deceptive trade practices in the course of its business, in violation of CCPA, Section 6-1-105(a), including:

a. Knowingly making a false representation as to the characteristics of services;

b. Representing that services are of a particular standard, quality, or grade, if Defendant knows or should know they are or were of another;

c. Advertising services with the intent not to sell them as advertised; and

d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

175. Accutech's deceptive acts, omissions, and conduct include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

176. Accutech had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' PII. This exclusive knowledge includes, but is not limited to, information that Accutech received through internal and other non-public audits and reviews that concluded that Accutech's security

policies were substandard and deficient, and that Plaintiff's and Class members' PII and other Accutech data was vulnerable.

177. Accutech also had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

178. Accutech also had exclusive knowledge about the length of time that it maintained individual's PII after they stopped using Accutech's services.

179. Accutech failed to disclose, and actively concealed, the material information it had regarding Accutech's deficient security policies and practices, and regarding the security of the sensitive PII and financial information. For example, even though Accutech has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' PII was vulnerable as a result, Accutech failed to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. Accutech also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former customers' PII and other records. Likewise, during the days and weeks following the Data Breach, Accutech failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

180. Accutech had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, it made affirmative statements that were inconsistent with the information it did not disclose, and because Accutech was in a fiduciary position by virtue of the fact that Accutech collected and maintained Plaintiff's and Class members' PII and financial information.

181. Accutech's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Accutech's data security and its ability to protect the confidentiality of current and former customers' PII.

182. Had Accutech disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Accutech would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Accutech received, maintained, and compiled Plaintiff's and Class members' PII without advising that Accutech's data security practices were insufficient to maintain the safety and confidentiality of their PII.

183. Accordingly, Plaintiff and Class members acted reasonably in relying on Accutech's misrepresentations and omissions, the truth of which they could not have discovered.

184. Accutech's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as the IDSBA, the CCPA and FTC Act.

185. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should have reasonably avoided.

186. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Accutech's deceptive acts and practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to Accutech as their clients, and with the understanding that Accutech would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Accutech and which is subject to further breaches so long as Accutech fails to undertake appropriate and adequate measures to protect data in its possession.

187. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Accutech from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VII –- Violation of State Data Breach Statutes
(By Plaintiff on behalf of the Class)

188. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

189. This count is brought on behalf of all Class members.

190. Accutech is a corporation that owns, maintains, and records PII, and computerized data including PII, about its customers' current and former customers, including Plaintiff and Class members.

191. Accutech is in possession of PII belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

192. Accutech failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

193. Accutech, knowing and/or reasonably believing that Plaintiff's and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members as required by following data breach statutes.

194. Accutech's failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.80, *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

195. As a result of Accutech's failure to reasonably safeguard Plaintiff's and Class members' PII, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Accutech's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VIII – Violation of State Consumer Protection Statutes
(On behalf of Plaintiff, the Class, and the Subclass)

196. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

197. This count is brought on behalf of all Class members.

198. Accutech is a "person" as defined in the relevant state consumer statutes.

199. Accutech engaged in the conduct alleged herein that was intended to result, and which did result, in the trade and commerce with Plaintiff and Class members. Accutech is engaged in, and its acts and omissions affect, trade and commerce. Further, Accutech's conduct implicates consumer protection concerns generally.

200. Accutech's acts, practices and omissions were done in the course of Accutech's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

201. Accutech's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act and similar state laws, rules, and regulations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and Class members that their PII was accessed by unauthorized persons in the Data Breach.

202. By engaging in such conduct and omissions of material facts, Accutech has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another", and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of

misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

203. Accutech's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Accutech's data security and ability to protect the confidentiality of PII.

204. Accutech intentionally, knowingly, and maliciously misled Plaintiff and Class members and induced them to rely on its misrepresentations and omissions.

205. Had Accutech disclosed that its data systems were not secure and, thus, vulnerable to attack, it would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Accutech received, maintained, and compiled Plaintiff's and Class members' PII without advising that Accutech's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and the Class members acted reasonably in relying on Accutech's misrepresentations and omissions, the truth of which they could not have discovered.

206. Past breaches within the industry and against Accutech itself put Accutech on notice that its security and privacy protections were inadequate.

207. Accutech's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like the IDSCPA, CCPA, and the FTC Act.

208. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

209. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of Accutech's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal and financial information entrusted to Defendant and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

210. Defendant's conduct described herein, including without limitation, Defendant's failure to maintain adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII, Defendant's failure to disclose the material fact that it did not have

adequate computer systems and safeguards to adequately protect Plaintiff's and Class members' PII, Defendant's failure to provide timely and accurate notice to of the material fact of the Data Breach, and Defendant's continued acceptance of Plaintiff's and Class members' PII constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq.*;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq*., and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq*.;

g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq.*;

i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq.*; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq.*;

j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq.*; and Idaho Code § 48-603C, *et seq.*;

k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq.*;

l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;

n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), e*t seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;

u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;

w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;

y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;

bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq*.;

dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq*.;

ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq*.;

gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq*.;

hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq*.; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq*.;

ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq*.;

jj. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq*.;

kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq*.;

ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq*.;

mm. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq*.;

nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);

oo. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq*.;

pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq*.;

rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq*.;

ss. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.;

uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and

vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

211. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT IX –- Intrusion Upon Seclusion
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

212. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

213. This count is brought on behalf of all Class members.

214. Plaintiff bring this claim on behalf of persons who reside in Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia; and any other state that recognizes a claim for intrusion upon seclusion under the facts and circumstances alleged above (the "Intrusion Upon Seclusion States").

215. Plaintiffs and Class members had a reasonable expectation of privacy in the PII that Accutech possessed and/or continues to possess.

216. By failing to keep Plaintiff's and Class members' PII safe, and by misusing and/or disclosing their PII to unauthorized parties for unauthorized use, Accutech invaded Plaintiff's and Class members' privacy by:

a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and

b. Publicizing private facts about Plaintiffs and Class members, which is highly offensive to a reasonable person.

217. Accutech knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's position would consider Accutech's actions highly offensive.

218. Accutech invaded Plaintiff's and Class member' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

219. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their PII was unduly frustrated and thwarted. Accutech conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

220. In failing to protect Plaintiff's and Class members' PII, and in misusing and/or disclosing their PII, Accutech has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class members' rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its many millions of customers. Plaintiff, therefore, seek an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

COUNT X –- Unjust Enrichment
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

221. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

222. This count is brought on behalf of all Class members.

223. Plaintiff and the Class have an interest, both equitable and legal, in their PII and financial information that was collected and maintained by Accutech.

224. Accutech was benefitted by the conferral upon it of Plaintiff's and Class members' PII and by its ability to retain and use that information. Accutech understood that it was in fact so benefitted.

225. Accutech also understood and appreciated that Plaintiff's and Class members' PII and financial was private and confidential and its value depended upon Accutech maintaining the privacy and confidentiality of that information.

226. But for Accutech's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provide or authorized their PII to be provided to Accutech, and Accutech would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining customers, gaining the reputational advantages conferred upon it by Plaintiff and Class members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

227. As a result of Accutech's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that PII) Accutech has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

228. Accutech's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

229. Under the common law doctrine of unjust enrichment, it is inequitable for Accutech to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Accutech's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

230. The benefit conferred upon, received, and enjoyed by Accutech was not conferred officiously or gratuitously, and it would be inequitable and unjust for Accutech to retain the benefit.

231. Accutech is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Accutech as a result of its wrongful conduct, including specifically the value to Accutech of the PII and financial information that was accessed and exfiltrated in the Data Breach and the profits Accutech receives from the use and sale of that information.

COUNT XI –- Declaratory Judgment
(By Plaintiff on behalf of the Class, or, in the alternative, the Colorado Subclass)

232. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

233. This count is brought on behalf of all Class members.

234. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described herein.

235. An actual controversy has arisen in the wake of the Data Breach regarding Accutech's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether Accutech is currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Accutech's data security measures remain inadequate.

236. Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

237. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Accutech continues to owe a legal duty to secure Plaintiff's and Class members' PII, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure PII.

238. The Court also should issue corresponding prospective injunctive relief requiring Accutech to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class members' PII.

239. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy. The threat of another breach of the PII in Accutech's possession, custody, and control is real, immediate, and substantial. If another breach of Accutech's network, systems, servers, or workstations occurs, Plaintiff and the Class will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

240. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Accutech if an injunction is issued. Among other things, if another massive data breach occurs at Accutech, Plaintiff and the Class will likely be subjected to substantial identify theft and

other damage. On the other hand, the cost to Accutech of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Accutech has a pre-existing legal obligation to employ such measures.

241. Issuance of the requested injunction will serve the public interest by preventing another data breach at Accutech, thus eliminating additional injuries to Plaintiff and the thousands of Class members whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Accutech, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and the Class members statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the putative Class, demand a trial by jury on all issues so triable.

Date: March 22, 2022

Respectfully Submitted,

/s/ *Gary M. Klinger*

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Daniel O. Herrera
Nickolas J. Hagman
Olivia Lawless
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class

*pro hac vice forthcoming