Patricia N. Syverson (CA SBN 203111)
BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
600 W. Broadway, Suite 900
San Diego, California 92101
Telephone: (602) 274-1100
psyverson@bffb.com

Norman E. Siegel (*pro hac vice* forthcoming)
J. Austin Moore (*pro hac vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

Additional Attorneys on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PHILLIP TORETTO and DANIEL C. KING, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

MEDIANT COMMUNICATIONS, INC., a Delaware corporation,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

1. **Negligence;**
2. **Negligence Per Se;**
3. **Breach of Contract;**
4. **Breach of Implied Contract;**
5. **Unjust Enrichment;**
6. **Declaratory Judgment;**
7. **Violation of California's Customer Records Act; and**
8. **Violation of California's Unfair Competition Law**

Plaintiffs Phillip Toretto and Daniel King, individually and on behalf of all persons similarly situated, bring this Class Action Complaint against Defendant Mediant Communications, Inc. ("Defendant" or "Mediant"), based upon personal knowledge with respect to themselves, and on information and belief derived from investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Mediant is a leading investor communications firm whose "pioneering use of technology helps companies improve shareholder and client relationships and safeguard regulatory compliance."[1] As relevant here, public companies and mutual funds hire Mediant as their proxy agent to distribute materials to shareholders, coordinate shareholder votes, and tabulate voting results. During this process, companies entrust Mediant with sensitive shareholder information in order to effectuate the distribution of materials and the coordination of important votes.

2. On April 1, 2019, hackers obtained unauthorized access to Mediant's business email accounts and exfiltrated the personal information of its customers' investors (the "Data Breach"). The stolen shareholder information included names, genders, physical addresses, email addresses, phone numbers, Social Security Numbers, tax identification numbers, account numbers, and various other types of information such as units owned, issue dates, and owner/annuitant designation (hereafter, collectively referred to as "Personal Information").

3. Mediant – a company that touts itself as employing cutting-edge technology – is responsible for allowing the breach to occur by failing to implement and maintain reasonable safeguards and failing to comply with industry-standard data security practices, contrary to the representations made in Mediant's privacy policy.

4. As a result of Mediant's failure to protect the information it was entrusted to safeguard, Plaintiffs and Class Members have been exposed to or are at a

[1] Mediant, Company Profile, https://mediantinc.com/about/ (last visited Aug. 13, 2019).

significant risk of identity theft, financial fraud, and other identity-related fraud into the indefinite future. Moreover, although Mediant discovered the breach the same day that it occurred, it waited almost two months before notifying impacted shareholders, thereby knowingly exposing vulnerable individuals to even further identity theft and fraud.

PARTIES

5. Plaintiff Phillip Toretto is a resident and citizen of Sausalito, California, whose Personal Information was compromised in the Data Breach.

6. Plaintiff Daniel C. King is a resident and citizen of Dover, New Jersey, whose Personal Information was compromised in the Data Breach.

7. Mediant is an investor communications and financial technology company headquartered in New York, New York, and incorporated under the laws of the State of Delaware.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332, the Class Action Fairness Act, because: (i) there are 100 or more class members; (ii) the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs; and (iii) there is minimal diversity because at least one plaintiff and one defendant are citizens of different states. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

9. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b)(1), (c)(2) because Mediant is subject to this Court's personal jurisdiction in this action. Among other things, Mediant conducts business in this District and collected the Personal Information of Plaintiff Toretto and Class Members who reside in this District, promising to protect that information – information which has now been compromised as a result of the Data Breach. Mediant purposefully directed its activities and consummated numerous transactions using the Personal Information of Class

Members who reside in this District, including Plaintiff Toretto, in the regular course of its business, thereby invoking the benefits and protections of California's laws. The claims alleged herein relate to Mediant's forum-related activities, including notifying California residents that they were victims of the Data Breach.

STATEMENT OF FACTS

A. The Data Breach

10. Mediant holds itself out as an "industry-leading investor communications solutions provider for banks, brokers, corporate issuers, funds, and investment advisors." In its marketing materials,[2] Mediant summarizes its offerings as follows:

WHAT WE DO

Mediant offers a wide range of solutions for the investor communications lifecycle, all via our single, integrated MIC platform. Whether you're a financial advisor or a back-office professional, our centralized platform gives you access to the real-time, actionable information you need.

MEDIANT PROVIDES A COMPREHENSIVE SUITE OF SOLUTIONS FOR:

PROXY
- Highly scalable print, electronic, and mail management
- Extensive data analytics, robust tabulation, and reporting
- End-to-end proxy meeting support

CORPORATE ACTIONS
- Custom-branded print and electronic corporate action communications
- Electronic corporate action documents and source materials stored online

REGULATORY REPORT DISTRIBUTION
- Robust in-house fulfillment for control over entire regulatory report distribution process
- Automated process and better insight and tracking

STATEMENTS & TRADE CONFIRMS
- Flexible, scalable management of statement and trade confirms
- Secure and on-time distribution and delivery

ANYTIME, ANYWHERE ACCESS
- Quick and easy electronic access to all of our solutions from any device

FULFILLMENT SERVICES
- Technology-enabled print, mail, and fulfillment services
- Secure facility successfully processes and distributes millions of investor communications documents each year

REGULATORY COMPLIANCE SERVICE
- Comprehensive business rules surrounding applicable regulatory requirements
- Regulatory updates and support from compliance specialists

TURN-KEY E-DELIVER & ARCHIVING
- SEC-compliant electronic delivery and document archive solution
- Streamlined e-consent process with custom, user-friendly sites

PROSPECTUS SERVICES
- Comprehensive in-house print and mail system for timely and efficient prospectus delivery
- Complete and compliant support for T+1 prospectus fulfillment, pre-sale delivery, combined confirms

[2] Mediant 2018 Proxy Guide, Corporate Issuer Services, https://www.proxydocs.com/branding/212121/2018/files/assets/common/downloads/Mediant%202018%20Annual%20Proxy%20Guide%20.pdf (last visited Aug. 13, 2019).

11. On information and belief, Mediant has numerous clients that reside or maintain their principal place of business in California.[3]

12. On April 1, 2019, hackers obtained unauthorized access to Mediant's business email accounts and exfiltrated the Personal Information of its customers' investors.

13. According to Mediant, it discovered the unauthorized access that same day and disconnected the affected server from the company's system. Mediant then commenced an investigation into the breach, but did not take any action at the time to notify either its impacted customers or their investors. Mediant has disclosed little else regarding the breach, including the method by which its accounts were compromised or how many individuals were affected.

14. At the end of May 2019, almost two full months after Mediant discovered the Data Breach, Mediant began notifying state attorneys general and sending notices to its customers' investors whose Personal Information had been stolen.

15. California law requires a business or state agency to notify any California resident whose unencrypted personal information, as defined, was acquired, or reasonably believed to have been acquired, by an unauthorized person. (*see* Cal. Civ. Code § 1798.82(a)). The law also requires that a sample copy of a breach notice sent to more than 500 California residents must be provided to the California Attorney General. On May 28, 2019, Mediant provided to the California Attorney General a sample notice indicating that numerous California residents were affected by the Data Breach.

[3] *See, e.g.*, Griffin-American Healthcare REIT III, Inc. Securities and Exchange Commission ("SEC") Schedule 14A at 2 ("Griffin-American Healthcare REIT III will bear the entire cost of the solicitation of proxies from its stockholders. We have retained Mediant Communications Inc. to assist us in the distribution of proxy materials and solicitation of votes. We anticipate paying Mediant Communications Inc. approximately $84,000 for such services.").

16. According to the sample notice, Mediant's notification letters contain a list of the company or companies from which the affected investors' information was stolen and a list of the specific types of Personal Information stolen from the investor during the Data Breach. For example, according to the specific notice for Jackson National Life Insurance Company posted on the California State Attorney General's website, the stolen investor information from that company included investors' full names, genders, physical addresses, email addresses, phone numbers, Social Security Numbers, tax identification numbers, account numbers, and various other specific types of information such as units owned, issue dates, and owner/annuitant designation.[4]

17. Sample notices posted to the websites of the Vermont and California Attorneys General explained that Mediant "provides many mutual funds and public companies, including real estate investment trusts, with mailing and document processing services as well as services in connection with their annual and special shareholder meetings, including the distribution of proxy materials, coordination of votes, and tabulation of voting results. Mutual funds and public companies hire proxy agents such as Mediant in connection with their shareholder meetings as a matter of standard practice."[5] Mediant disclosed that it received the shareholders' information "while providing its services to entities related to [the affected person's] ownership of certain securities."

---

[4] State of California Department of Justice, *Jackson National Life Insurance Company Notice*, https://oag.ca.gov/system/files/CA%20Consumer%20Notice_Mediant_Sample_0.pdf# (last visited Aug. 13, 2019).

[5] *See, e.g.*, Office of the Vermont Attorney General, *Notice of Data Breach*, https://ago.vermont.gov/blog/2019/05/31/mediant-communications-sbn-to-consumers/ (last visited Aug. 13, 2019); *see also* State of California Department of Justice, *Submitted Breach Notification Sample*, https://www.oag.ca.gov/system/files/L01_Mediant_%20General_0.pdf (last visited Aug. 13, 2019); State of California Department of Justice, Jackson National Life Insurance Company Notice, https://oag.ca.gov/system/files/CA%20Consumer%20Notice_Mediant_Sample_0.pdf# (last visited Aug. 13, 2019).

18. After providing a cursory recitation of the facts surrounding the Data Breach, Mediant stated that on May 10, 2019 it had "determined [the recipient shareholder's] personal information was among the information impacted." Yet, instead of immediately notifying affected individuals, Mediant "first informed" the companies whose shareholders were impacted – two weeks prior to notifying the shareholders themselves.

19. Mediant represented that none of the companies who provided investor information had systems involved in the incident or "were otherwise at fault in the incident."

20. All of the sample notices represented that Mediant has "taken steps to strengthen [its] protection of personal information, including updating our network security controls and email systems."[6] Mediant provided no explanation as to why its network security controls and email systems were not sufficiently updated prior to a malicious and unauthorized party gaining access to extremely sensitive Personal Information of its customers' investors.

21. Mediant further stated that it will "continue to closely monitor and take further steps to safeguard such information"; had "reported the matter to law enforcement, but this notice has not been delayed because of law enforcement investigation"; and is "offering credit monitoring for a period of 24 months at no cost to [the impacted investors]."

22. Mediant recommended that the affected investors take steps themselves to prevent fraud and identity theft, telling them to "closely review or monitor [their] financial accounts, statements, credit reports and other financial information for any evidence of unusual activity, fraudulent charges or signs of identity theft." The notice attaches three pages containing "additional information" regarding steps the affected investors can take, including implementing security freezes and fraud alerts and

[6] *See* State of California Department of Justice, *Submitted Breach Notification Sample*, https://www.oag.ca.gov/system/files/L01_Mediant_%20General_0.pdf (last visited Aug. 13, 2019).

providing the contact information for certain state attorneys general who can provide additional information about "steps [the affected investors] can take to prevent identity theft."

23. Unfortunately, Mediant's notification to affected individuals was severely deficient in that it: (1) failed to disclose precisely how Mediant obtained affected individuals' information; (2) failed to disclose precisely how the Data Breach occurred, including the method by which its email accounts were accessed or the information exfiltrated; (3) failed to disclose how many people were affected; (4) failed to disclose who was responsible for the Data Breach and how many unauthorized individuals had access to the stolen information; and (5) failed to disclose the results of any investigations into the Data Breach.

24. By keeping affected individuals in the dark about the key details surrounding the Data Breach, Mediant has prevented affected individuals from taking meaningful, proactive, and targeted mitigation measures that could help protect them against severe harm.

B. Plaintiff Toretto's Allegations

25. Following the Data Breach, Plaintiff Toretto received a letter from Mediant dated May 31, 2019 stating that his Personal Information had been compromised during the Data Breach.

26. Specifically, the letter stated that "Mediant received your personal information while providing its services to entities related to your ownership of certain securities including: Blackstone Real Estate Income Trust, Inc. (2017 annual meeting)." The letter disclosed that Plaintiff Toretto had the following information compromised: "your name, address, email address, phone number, Social Security Number/tax identification numbers, and transfer agent's account ID."

27. The letter advised Plaintiff Toretto to "be vigilant and closely review or monitor your financial accounts, statements, credit reports and other financial

information for any evidence of unusual activity, fraudulent charges, or signs of identity theft."

28. As a result of the Data Breach, Plaintiff Toretto has expended time and effort regularly monitoring his financial and credit accounts in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff Toretto remains at a substantial and imminent risk of future harm.

C. Plaintiff King's Allegations

29. Following the Data Breach, Plaintiff King received a letter from Mediant dated May 31, 2019 stating that his Personal Information had been compromised during the Data Breach.

30. Specifically, the letter stated that "Mediant received your personal information while providing its services to entities related to your ownership of certain securities including: Ivy Natural Resources Fund's 2019 proxy." The letter disclosed that Plaintiff King had the following information compromised: "your name, address, Social Security Number/tax ID number, and transfer agent's account ID."

31. The letter advised Plaintiff King to "be vigilant and closely review or monitor your financial accounts, statements, credit reports and other financial information for any evidence of unusual actively, fraudulent charges, or signs of identity theft."

32. As a result of the Data Breach, Plaintiff King has expended time and effort regularly monitoring his financial and credit accounts in order to mitigate against potential harm. Given the highly-sensitive nature of the information stolen, Plaintiff King remains at a substantial and imminent risk of future harm.

D. Mediant Knew it was a Target of Cyber-Threats

33. Mediant prides itself on its "pioneering use of technology," which "helps companies improve shareholder and client relationships and safeguard regulatory compliance."[7]

[7] Mediant, *Company Profile*, https://mediantinc.com/about/ (last visited Aug. 13, 2019).

34. On its website, Mediant advertises to potential customers by touting its "web-based technology" and "industry-leading security." Mediant represents that it maintains a "Comprehensive cybersecurity program with highly robust, redundant infrastructure platform that provides reliability and security you need."[8] It further states that, "We undergo annual audits and comply with all federal, state, and industry privacy and security regulations."[9]

35. In its Privacy Policy published on its website and available to all of its customers' investors, Mediant states that it is committed to maintaining the privacy of shareholders' Personal Information, which Mediant defines to include names, account numbers, physical addresses, e-mail addresses, the number of shares that you own, and other information that can be used to identify the person. Mediant promises that personally identifiable data "provided to Mediant by you or by third parties will be kept confidential."[10]

36. Further, Mediant represents that it "maintains physical, electronic and procedural safeguards in accordance with laws and regulations governing confidentiality and security of information. Access to personal information is limited to only those workers and third parties who need access to the information to perform necessary activities for Mediant. We also provide security for your information by maintaining servers that are secure and dedicated solely to the services that we provide to protect against loss, misuse, or alteration of your information."[11]

37. As a financial technology firm that purports to develop "game-changing new technologies for the investor communications ecosystem,"[12] Mediant is fully

---

[8] Mediant, *Technology*, https://mediantinc.com/why-mediant/technology/ (last visited Aug. 13, 2019).

[9] *Id.*

[10] Mediant, *Privacy Policy*, https://mediantinc.com/privacy-policy/ (last visited Aug. 13, 2019).

[11] *Id.*

[12] Mediant, *MIC Platform*, https://mediantinc.com/solutions/mic-platform/ (last visited Aug. 13, 2019).

aware of the dangers data breaches pose to companies who compile investor information. In fact, Mediant's Chief Technology Officer (CTO), Stacey Robinson, wrote an article in 2017 specifically addressing the severe threat cyber-attacks pose to the financial industry and companies like Mediant. The article, entitled "Cyber Attacks May Make Financial Industry 'WannaCry,"[13] is posted on Mediant's website and was published at WealthManagement.com.

38. In the article, Mediant's CTO recognized that "[l]arge-scale cybersecurity breaches are in the news on a weekly and even daily basis" and that the "financial services industry is a huge target for cybercriminals — more than any other industry — and the risk has evolved from financial theft and fraud to more complex and serious consequences like theft of intellectual property, business disruption and reputation damage (Deloitte). In other words, hackers are not just stealing lists of Social Security numbers anymore, but rather executing serious breaches with more far-reaching consequences."[14]

39. Mediant's CTO explained that "at financial services firms, cyberattacks exploit flaws in security programs that allow threat actors to gain access. Among the most common attack targets are endpoints, such as laptops, tablets and smartphones. Endpoints are particularly vulnerable because they require both robust security protocols and effective education for the firms' employees, who act as the last line of defense. Attackers use weaponized email attachments and links to attack sites in order to compromise credentials and establish a foothold on the endpoint. The 2016 Data Breach Investigations Report (DBIR) from Verizon points out that it only takes

[13] Robinson, Stacey, Cyber Attacks May Make Financial Industry "WannaCry," Wealth Management (May 24, 2017),https://www.wealthmanagement.com/technology/cyber-attacks-may-make-financial-industry-wannacry; *see also* https://mediantinc.com/cyber-attacks-financial-services-industry (last visited Aug. 13, 2019).

[14] *Id.*

minutes to compromise a host and collect a set of valid credentials, and in most cases, data exfiltration is underway just days after compromise."[15]

40. Mediant's CTO described why "endpoints," such as email accounts are especially vulnerable: "Compromising an endpoint gives the attacker a lot of bang for their buck, since they provide easy access to additional data and systems. One of the most effective ways to exploit endpoint security vulnerability is via phishing, a form of social engineering that commonly targets financial services companies. Per the DBIR, 30 percent of phishing emails were opened and 12 percent clicked on the malicious attachment or link, thereby enabling the attack."[16]

41. Mediant's CTO also acknowledged that cyber-attacks can be prevented: "Successful endpoint security is a complex endeavor, requiring an extensive framework and consistent attention. It requires quality and maturity in areas such as OS hardening, the principle of least privilege and patching. Particular consideration should be paid to advanced security solutions around application whitelisting, exploit detection and prevention, device blocking, firewalls, web filtering and malware prevention. While attackers will continue to use phishing as an attack vector in order to capitalize on human error, it's certainly possible — and these days, essential — to develop and implement a robust security framework that accounts for all vulnerabilities."[17]

42. As acknowledged by Mediant's CTO and reflected in its Privacy Policy, Mediant was at all times fully aware of its obligation to protect investors' Personal Information and the risks associated with failing to do so. Indeed, Mediant observed frequent public announcements of data breaches affecting financial industries and knew that information of the type collected, maintained, and stored by Mediant is highly coveted and a frequent target of hackers.

---

[15] *Id.*

[16] *Id.*

[17] *Id.*

43. Indeed, a February 2018 report prepared by the Identity Theft Resource Center (ITRC) noted that, "For years, the financial services sector globally has been a primary target for attacks by cybercriminals largely because of the tremendous value of the information available. In fact, financial services firms are reportedly hit by security incidents a staggering 300 times more frequently than businesses in other industries. This startling statistic underscores the importance of financial services professionals being aware of the breadth and causes of successful cyberattacks and also their need to keep their knowledge of risk mitigation strategies current."[18]

44. In its 2019 Data Breach Investigations Report, Verizon noted that there were 927 breaches affecting the insurance and financial industries in 2018 alone, with confirmed data disclosure in 207 of the breaches.[19] The report found that 71% of breaches are "financially motivated" meaning the hackers accessed information with the intention to profit from it.

45. Mediant also observed numerous other well-publicized data breaches involving major corporations that were targeted given the sensitive consumer information they retained. For example, in early 2015, Anthem, Inc., the second-largest health insurer in the United States, suffered a massive data breach exposing the names, addresses, Social Security numbers, dates of birth, and employment histories of nearly 80 million current and former plan members nationwide.[20]

46. In March 2015, health insurer Premera Blue Cross announced it suffered a data breach that exposed the medical data and financial information of 11 million customers, including claims data, clinical information, banking account numbers,

---

[18] ITRC, *The Impact of Cybersecurity Incidents on Financial Institutions* (Feb. 2018), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_Generali_The-Impact-of-Cybersecurity-Incidents-on-Financial-Institutions-2018.pdf (last visited Aug. 13, 2019).

[19] Verizon, *2019 Data Breach Investigations Report*, available with subscription at: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

[20] C. Riley, *Insurance Giant Anthem Hit by Massive Data Breach*, CNN (Feb. 6, 2015), https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/ (last visited Aug. 13, 2019).

Social Security numbers, birth dates and other data in an attack that began in May 2014.[21] Shortly thereafter, New York-based insurer Excellus BlueCross BlueShield announced a breach that exposed the personal information of 10 million of its plan members in an attack dating back to 2013.[22]

47. Through a series of data breaches extending back to 2013, more than three billion Yahoo! user accounts were compromised when users' names, addresses, and dates of birth were stolen.[23]

48. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target and the Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.[24]

49. In September 2017, credit reporting agency Equifax announced that hackers stole the personal and financial information of 147 million Americans between May and July 2017.[25] The following year, hotel giant Marriott announced that 383 million guest records were exfiltrated from its hotel guest reservation database over a four-year period.[26]

---

[21] *Premera Blue Cross Says Data Breach Exposed Medical Data*, THE NEW YORK TIMES (March 1, 2015), https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/ (last visited Aug. 13, 2019).

[22] *Cyber Breach Hits 10 Million Excellus Healthcare Customers*, USA TODAY (Sept. 10, 2015), https://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/ (last visited Aug. 13, 2019).

[23] S. Larson, *Every Single Yahoo Account was Hacked – 3 Billion in All*, CNN (OCT. 4, 2017), https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html (last visited Aug. 13, 2019).

[24] B. Krebs, *Home Depot Hit By Same Malware as Target*, KREBS ON SECURITY (Sept. 14, 2014), https://krebsonsecurity.com/tag/home-depot-databreach/ (last visited Aug. 13, 2019).

[25] Equifax 2017 Cybersecurity Incident & Important Consumer Information, https://www.equifaxsecurity2017.com/frequently-asked-questions/ (last visited Aug. 13, 2019).

[26] Marriott Provides Update on Starwood Database Security Incident, https://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/ (last visited Aug. 13, 2019).

50. Despite being a holder of Personal Information for thousands of individuals nationwide, Mediant failed to prioritize data security by adopting reasonable data resources security measures to prevent and detect unauthorized access to its databases. Mediant had the resources to prevent a breach and made significant expenditures to promote its services, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches affecting financial and other related industries.

E. Mediant Failed to Comply with Regulatory Guidance

51. Federal agencies have issued recommendations and guidelines to temper data breaches and the resulting harm to individuals and financial institutions. For example, the Federal Trade Commission ("FTC") has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[27]

52. 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.[28] Among other things, the guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the

[27] Federal Trade Commission, *Start With Security* (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Aug. 13, 2019).

[28] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Aug. 13, 2019).

system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[29]

53. Additionally, the FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[30]

54. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[31]

55. In this case, Mediant was fully aware of its obligation to use reasonable measures to protect the personal information of its customers, acknowledging as much in its own privacy policy. Mediant also knew it was a target for hackers. But despite understanding the consequences of inadequate data security, Mediant failed to comply with industry-standard data security requirements.

56. Mediant's failure to employ reasonable and appropriate measures to protect against unauthorized access to members' information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

F. The Impact of the Data Breach on Affected Individuals

57. Given the sensitive nature of the Personal Information stolen in the Data Breach –including names, genders, physical addresses, email addresses, phone

---

[29] *Id.*

[30] FTC, *Start With Security*, *supra* note 27.

[31] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Aug. 13, 2019).

numbers, Social Security Numbers, tax identification numbers, account numbers, and various other types of information such as units owned, issue dates, and owner/annuitant designation – hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future.

58. In fact, many victims of the Data Breach have likely already experienced harms as the result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud, unauthorized lines of credit opened in their names, medical and healthcare fraud, and unauthorized access to their bank accounts. Plaintiffs and Class Members have also spent time, money, and effort dealing with the fallout of the Data Breach, including purchasing credit protection services, contacting their financial institutions, checking credit reports, and spending time and effort searching for unauthorized activity.

59. The Personal Information exposed in the Data Breach is highly-coveted and valuable on underground or black markets. For example, a cyber "black market" exists in which criminals openly post and sell stolen consumer information on underground internet websites known as the "dark web" – exposing consumers to identity theft and fraud for years to come. Identity thieves can use the Personal Information to: (a) create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d) obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any number of other frauds, such as obtaining a job, procuring housing, or giving false information to police during an arrest.

60. And, the impact of identity theft can have ripple effects, which can adversely affect the future financial trajectories of victims' lives. For example, the

Identity Theft Resource Center reports that respondents to their surveys in 2013-2016 described that the identity theft they experienced affected their ability to get credit cards and obtain loans, such as student loans or mortgages.[32] For some victims, this could mean the difference between going to college or not, becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-interest loan.

61. It is no wonder then that identity theft exacts a severe emotional toll on its victims. The 2017 Identity Theft Resource Center survey evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed
- 67% reported anxiety
- 66% reported feelings of fear related to personal financial safety
- 37% reported fearing for the financial safety of family members
- 24% reported fear for their physical safety
- 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft
- 7% reported feeling suicidal.[33]

62. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from their experience with identity theft:

- 48.3% of respondents reported sleep disturbances
- 37.1% reported an inability to concentrate / lack of focus
- 28.7% reported they were unable to go to work because of physical symptoms
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues)
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[34]

---

[32] Identity Theft Resource Center, *The Aftermath 2017*, https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf (last visited Aug. 13, 2019).

[33] *Id.*

63. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[35]

64. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.

---

[34] *Id.*

[35] FTC, *Combating Identity Theft A Strategic Plan* (April 2007), https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf (last visited Aug. 13, 2019).

> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[36]

65. As the result of the wide variety of injuries that can be traced to the Data Breach, Plaintiffs and Class Members have and will continue to suffer economic loss and other actual harm for which they are entitled to damages, including, but not limited to, the following:

a. purchasing services they would not have otherwise paid for and/or paying more for services than they otherwise would have paid, had they known the truth about Mediant's sub-standard data security practices;

b. losing the inherent value of their Personal Information;

c. losing the value of the explicit and implicit promises of data security;

d. identity theft and fraud resulting from the theft of their Personal Information;

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

f. costs associated with purchasing credit monitoring, credit freezes, and identity theft protection services;

g. unauthorized charges and loss of use of and access to their financial account funds and costs associated with 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;

h. lowered credit scores resulting from credit inquiries following fraudulent activities;

i. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to

[36] Social Security Administration, *Identity Theft and Your Social Security Number* (June 2017), http://www.ssa.gov/pubs/10064.html (last visited Aug. 13, 2019).

mitigate and address the actual and future consequences of the Data Breach, including discovering fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposing withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with the repercussions of the Data Breach; and

j. the continued imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being in the possession of one or many unauthorized third parties.

66. Even in instances where a consumer is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement that is not refunded. The Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" relating to identity theft or fraud.[37]

67. There may also be a significant time lag between when personal information is stolen and when it is actually misused. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

68. Plaintiffs and Class Members place significant value in data security. According to a recent survey conducted by cyber-security company FireEye, approximately 50% of consumers consider data security to be a main or important

[37] E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Aug. 13, 2019).

[38] U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Aug. 13, 2019).

consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less personal information to organizations that suffered a data breach.[39]

69. Because of the value consumers place on data privacy and security, companies with robust data security practices can command higher prices than those who do not. Indeed, if consumers did not value their data security and privacy, Mediant would have no reason to tout its data security efforts to their actual and potential customers.

70. As a direct result of Mediant's failure to protect the Personal Information it was entrusted to safeguard, Plaintiffs and Class Members have been placed at an imminent and continuing increased risk of harm from identity theft and identity fraud, requiring them to spend time, money, and effort to mitigate the actual and potential impact of the Data Breach on their lives including, but limited to, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity.

71. Further, Mediant continues to hold Plaintiffs' and Class Members' Personal Information, and, therefore, they have an interest in ensuring that their Personal Information is secured and not subject to further theft.

CLASS ALLEGATIONS

72. Plaintiffs seek relief on behalf of themselves and as representatives of all others who are similarly situated. Pursuant to Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a nationwide class defined as follows:

---

[39] FireEye, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 2016), https://www.fireeye.com/blog/executive-perspective/2016/05/beyond_the_bottomli.html (last visited Aug. 13, 2019).

> All persons in the United States whose Personal Information was compromised as a result of the data breach experienced by Mediant on or around April 1, 2019 (the "Class" or "Nationwide Class").

73. Pursuant to Rule 23, Plaintiff Toretto asserts claims under the law of California on behalf of a separate statewide subclass defined as follows:

> All persons in the State of California whose Personal Information was compromised as a result of the data breach experienced by Mediant on or around April 1, 2019 (the "California Subclass").

74. Pursuant to Rule 23, and in the alternative to the Nationwide Class, Plaintiff King asserts claims under the law of New Jersey on behalf of a separate statewide subclass defined as follows:

> All persons in the State of New Jersey whose Personal Information was compromised as a result of the data breach experienced by Mediant on or around April 1, 2019 (the "California Subclass").

75. Excluded from each of the above Classes is Mediant, any entity in which Mediant has a controlling interest, and Mediant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded are all persons who make a timely election to be excluded from the Class and any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

76. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

77. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

78. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class Members is unknown

to Plaintiffs at this time, the proposed Class includes potentially hundreds of thousands of individuals whose Personal Information was compromised in the Data Breach. Class members may be identified through objective means. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

79. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class Members. The predominating common questions include:

a. Whether Mediant had a duty to protect Personal Information;

b. Whether Mediant's security measures to protect its data systems were reasonable in light of known legal requirements;

c. Whether Mediant's security measures to protect its data systems were reasonable in light of known industry standards;

d. Whether Mediant's failure to implement adequate data security measures allowed the breach of its data systems to occur;

e. Whether Mediant's conduct constituted unfair or deceptive trade practices;

f. Whether Mediant's conduct was the proximate cause of the Data Breach and/or the loss of the Personal Information of Plaintiffs and Class Members;

g. Whether Plaintiffs and Class Members were injured and suffered damages or other losses because of Mediant's failure to reasonably protect its data systems and data network; and,

h. Whether Plaintiffs and Class members are entitled to relief.

80. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiffs' claims are typical of those of other Class Members. Plaintiffs' Personal

Information was in Mediant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiffs' damages and injuries are akin to other Class Members' damages and injuries, and Plaintiffs seek relief consistent with the relief of the Class.

81. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiffs are adequate representatives of the Class because they are members of the Class and are committed to pursuing this matter against Mediant to obtain relief for the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, and have extensive experience litigating data breach and privacy class actions. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

82. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Mediant, and thus, individual litigation to redress Mediant's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

83. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Mediant, through its uniform conduct, acted

or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

84. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Mediant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Mediant failed to take commercially reasonable steps to safeguard the Personal Information of Plaintiffs and the Class Members;

c. Whether Mediant's security measures to protect is systems were reasonable in light of known legal requirements; and,

d. Whether adherence to FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

85. Finally, all members of the proposed Class are readily ascertainable. Mediant has access to information regarding which individuals were affected by the Data Breach. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice to the Class.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses)

86. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

87. Mediant collected and stored the Personal Information of Plaintiffs and Class Members for commercial gain, and promised Plaintiffs and Class Members in its Privacy Policy that it would keep their information safe.

88. Mediant owed a duty to Plaintiffs and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiffs' and Class Members' Personal Information within its control from being compromised, lost, stolen, accessed and misused by unauthorized persons.

89. Mediant also owed a duty of care to Plaintiffs and members of the Class to provide security of their Personal Information consistent with industry standards.

90. Mediant's duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. Mediant's duty to use reasonable care in protecting Personal Information is also required by common law, statutes and regulations such as the FTC Act, as well as its own promises regarding privacy and data security.

91. Mediant knew, or should have known, of the risks inherent in collecting and storing Personal Information and the importance of adequate, industry-standard, and up-to-date security.

92. Mediant breached its common law, statutory, and other duties to Plaintiffs and Class Members in numerous ways, including by:

a. failing to implement security systems, protocols and practices sufficient to protect Plaintiffs' and Class Members' Personal Information;

b. failing to comply with industry data security standards;

c. failing to comply with statutory and regulatory Personal Information safeguards; and,

d. failing to timely disclose that Plaintiffs' and Class members' Personal Information had been improperly acquired or accessed.

93. Mediant's failure to implement proper security measures to protect the sensitive Personal Information of Plaintiffs and Class Members as described in this

Complaint, created conditions conducive to a foreseeable, intentional criminal act – the unauthorized access of the Personal Information of Plaintiffs and Class Members.

94. It was also foreseeable that Mediant's failure to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class Members.

95. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Personal Information as described in this Complaint.

96. As a direct and proximate result of Mediant's conduct, Plaintiffs and the Class have and will suffer damages including, but not limited to: (i) the loss of the opportunity to determine for themselves how their Personal Information is used; (ii) the publication and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Personal Information, which remains in Mediant's possession and is subject to further unauthorized disclosures so long as Mediant fails to undertake appropriate and adequate measures to protect the Personal Information of its clients' investors in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Personal Information for the rest of their lives.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses)

97. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

98. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Mediant, of failing to use reasonable measures to protect Personal Information. 15 U.S.C. § 45(a)(1).

99. Mediant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' Personal Information and by failing to comply with applicable industry standards. Mediant's conduct was particularly unreasonable given the sensitive nature of the Personal Information it obtained and stored.

100. Mediant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

101. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

102. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

103. As a direct and proximate result of Mediant's negligence *per se*, Plaintiffs and Class Members have suffered, continue to suffer, and will suffer, injuries, damages, and harm as set forth herein.

COUNT III
BREACH OF CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses)

104. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

105. Mediant's Privacy Policy is an agreement between Mediant and individuals who provided their personal information to Mediant, whether directly or indirectly, including Plaintiffs and Class Members.

106. Mediant's Privacy Policy states, among other things, that Personal Information "provided to Mediant by you or by third parties will be kept confidential."

107. Mediant agreed it would (a) "maintain[] physical, electronic and procedural safeguards in accordance with laws and regulations governing confidentiality and security of information"; (b) restrict "[a]ccess to personal information … to only those workers and third parties who need access to the information to perform necessary activities for Mediant"; and (c) "provide security for your information by maintaining servers that are secure and dedicated solely to the services that we provide to protect against loss, misuse, or alteration of your information."

108. Plaintiffs and Class Members formed a contract with Mediant when they provided Personal Information to Mediant, whether directly or indirectly, subject to the Privacy Policy.

109. Mediant breached its agreement with Plaintiffs and Class Members by failing to protect their Personal Information, including failing to comply with the promises and obligations set forth in the Privacy Policy.

110. As a direct and proximate result of Mediant's breach, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

COUNT IV
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses)

111. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

112. Plaintiffs and Class Members directly and indirectly provided their Personal Information to Mediant in order to purchase securities.

113. As part of these transactions, Mediant agreed to safeguard and protect the Personal Information of Plaintiffs and Class Members. Implicit in the agreements between Mediant and Class Members was the obligation that Mediant would use the Personal Information for approved business purposes only and would not make unauthorized disclosures of the information or allow unauthorized access to the information.

114. Additionally, Mediant implicitly promised to retain this Personal Information only under conditions that kept such information secure and confidential and therefore had a duty to reasonably safeguard and protect the Personal Information of Plaintiffs and Class Members from unauthorized disclosure or access.

115. Plaintiffs and Class Members entered into implied contracts with the reasonable expectation that Mediant's data security practices and policies were reasonable and consistent with industry standards.

116. Plaintiffs and Class Members would not have directly or indirectly provided and entrusted their Personal Information to Mediant in the absence of the implied contract with Mediant. The safeguarding of Plaintiffs and Class Members' Personal Information was critical to realize the intent of the parties.

117. Mediant breached its implied contract with Plaintiffs and Class Members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' Personal Information, which was compromised as a result of the Data Breach.

118. Mediant's acts and omissions have materially affected the intended purpose of the implied contracts.

119. As a direct and proximate result of Mediant's breaches, Plaintiffs and Class Members sustained actual losses and damages as described in detail herein.

COUNT V
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, or, Alternatively, Plaintiffs and their respective Subclasses)

120. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein, and assert this claim in the alternative to their breach of contract claims to the extent necessary.

121. Plaintiffs and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Mediant and which was ultimately stolen in the Data Breach.

122. Mediant was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiffs and Class members and by its ability to retain and use that information.

123. Mediant appreciated and had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

124. Mediant also understood and appreciated that the Personal Information pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Mediant maintaining the privacy and confidentiality of that Personal Information.

125. But for Mediant's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and

entrusted with Mediant. Further, if Mediant had disclosed that its data security measures were inadequate, Mediant would not have been permitted to continue in operation by regulators, its clients, and participants in the marketplace.

126. As a result of Mediant's wrongful conduct as alleged herein, Mediant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class Members. Among other things, Mediant continues to benefit and profit from using Personal Information in the regular course of its business while its value to Plaintiffs and Class Members has been diminished.

127. Mediant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class Member's sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

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

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

130. Mediant is therefore liable to Plaintiffs and Class Members for restitution in the amount of the benefit conferred on Mediant as a result of its wrongful conduct, including specifically the value to Mediant of the Personal Information that was stolen in the Data Breach and the profits Mediant is receiving from the use of that information in the course of its business.

COUNT VI
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

131. Plaintiffs restate and re-allege the preceding paragraphs as if fully set forth herein.

132. Mediant, who promised in its Privacy Policy that it would protect Plaintiffs' and Class Members' Personal Information collected from Mediant's customers, still possesses the now-compromised Personal Information.

133. Mediant has only superficially represented to Plaintiffs and the Class that it has made unspecified "updates" remedying the as-yet unannounced security issue(s) that allowed hackers to obtain Plaintiffs' and Class Members' Personal Information via Mediant's business email accounts. Mediant has provided no assurances that Plaintiffs' and Class Members' information is actually safe, or that it has been deleted from Mediant's systems if it is no longer needed.

134. Accordingly, Mediant has not satisfied its obligations and legal duties to Plaintiffs and the Class. In fact, now that Mediant's lax approach towards data security has become public, the information in its possession is more vulnerable than it was prior to announcement of the Data Breach.

135. 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 state and federal statutes described in this Complaint.

136. An actual controversy has arisen in the wake of the Data Breach regarding Mediant's present and prospective common law and other duties to reasonably safeguard Personal Information and whether Mediant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Personal Information. Plaintiffs allege that Mediant's data security measures remain inadequate. Furthermore,

Plaintiffs continue to suffer injuries as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

137. Pursuant to the Declaratory Judgment Act, Plaintiffs seek a declaration that: (a) Mediant's existing data security measures do not comply with its obligations and duties of care; and (b) in order to comply with its obligations and duties of care, Mediant must: (i) purge, delete, or destroy in a reasonably secure manner Plaintiffs' and Class Members' Personal Information if it is no longer needed in order to prevent further theft; and (ii) implement and maintain reasonable, industry-standard security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Mediant's systems on a periodic basis, and ordering Mediant to promptly correct any problems or issues detected by such third-party security auditors;
b. engaging third-party security auditors and internal personnel to run automated security monitoring;
c. auditing, testing, and training its security personnel regarding any new or modified procedures;
d. segmenting Personal Information by, among other things, creating firewalls and access controls so that if one area of Mediant's systems is compromised, hackers cannot gain access to other portions of Mediant's systems;
e. purging, deleting, and destroying in a reasonable secure manner Personal Information not necessary for its provisions of services;
f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Mediant customers must take to protect themselves.

COUNT VII
VIOLATION OF CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq*.
(On Behalf of Plaintiff Toretto and the California Subclass)

138. Plaintiff Toretto restates and re-alleges the preceding paragraphs as if fully set forth herein.

139. Plaintiff Toretto and California Subclass Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Mediant and which was ultimately stolen in the Data Breach.

140. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

141. Mediant is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff Toretto and California Subclass Members.

142. Businesses that own or license computerized data that includes Personal Information are required to notify California residents when their Personal

Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must describe "what happened" and include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

143. Mediant is a business that owns or licenses computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

144. Plaintiff Toretto and California Subclass Members' Personal Information includes Personal Information as covered by Cal. Civ. Code § 1798.82.

145. Because Mediant reasonably believed that Plaintiff Toretto's and California Subclass Members' Personal Information was acquired by unauthorized persons during the Data Breach, Mediant had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

146. By failing to disclose the Data Breach in a timely and accurate manner, Mediant violated Cal. Civ. Code § 1798.82.

147. As a direct and proximate result of Mediant's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff Toretto and California Subclass Members suffered damages, as described above.

148. Plaintiff Toretto and California Subclass Members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT VIII
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff Toretto and the California Subclass)

149. Plaintiff Toretto restates and re-alleges the preceding paragraphs as if fully set forth herein.

150. Mediant is a "person" as defined by Cal. Bus. & Prof. Code §17201.

151. Mediant violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

152. Mediant's "unfair" acts and practices include:

a. Mediant failed to implement and maintain reasonable security measures to protect Plaintiff Toretto's and California Subclass Members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. Mediant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Toretto and the California Subclass, whose Personal Information has been compromised.

b. Mediant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' information and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. Mediant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Mediant's inadequate security, affected individuals could not have reasonably avoided the harms that Mediant caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

153. Mediant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§

1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq*., the FTC Act, 15 U.S.C. § 45, and California common law.

154. Mediant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Toretto and California Subclass Members' Personal Information, which were direct and proximate causes 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, 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 Toretto and California Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Toretto's and California Subclass Members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Toretto's and California Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Toretto's and California Subclass Members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Toretto's and California Subclass Members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.

155. Mediant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Mediant's data security and ability to protect the confidentiality of consumers' Personal Information.

156. As a direct and proximate result of Mediant's unfair, unlawful, and fraudulent acts and practices, Plaintiff Toretto and California Subclass Members were injured and lost money or property, the premiums and/or price received by Mediant for its goods and services, the loss of the benefit of their bargain with Mediant; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Personal Information; and an increased, imminent risk of fraud and identity theft.

157. Mediant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Toretto and California Subclass Members' rights. Mediant's acknowledgement of numerous breaches within the financial industry put it on notice that its security and privacy protections were inadequate.

158. Plaintiff Toretto and California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from

Mediant's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members proposed in this Complaint, respectfully request that the Court enter judgment in his favor and against Mediant as follows:

A. For an Order certifying the Classes, as defined herein, and appointing Plaintiffs as the class representatives and the undersigned counsel as class counsel;

B. For equitable relief enjoining Mediant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Personal Information;

C. For equitable relief compelling Mediant to use industry-standard security methods and policies with respect to data collection, storage and protection and to dispose of Plaintiffs' and Class Members' Personal information in its possession as soon as it is no longer needed;

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

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

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a jury trial on all issues so triable.

Dated: August 21, 2019

/s/ *Patricia N. Syverson*
Patricia N. Syverson (CA SBN 203111)
BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
600 W. Broadway, Suite 900
San Diego, California 92101
Telephone: (602) 274-1100
psyverson@bffb.com

Norman E. Siegel (*pro hac vice* forthcoming)
J. Austin Moore (*pro hac vice* forthcoming)
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
moore@stuevesiegel.com

Elaine A. Ryan (*pro hac vice* forthcoming)
Carrie A. Laliberte (*pro hac vice* forthcoming)
BONNETT, FAIRBOURN, FRIEDMAN & BALINT, P.C.
2325 E. Camelback Road, #300
Phoenix, Arizona 85016
Telephone: (602) 274-1100
eryan@bffb.com
claliberte@bffb.com

Counsel for Plaintiff and the Class