UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF OHIO
WESTERN DIVISION AT TOLEDO

CHRISTOPHER MASALES, individually and on behalf of all others similarly situated,
22923 US Highway 20A
Archbold, OH 43502

AND

PATRICIA MASALES, individually and on behalf of all others similarly situated,
22923 US Highway 20A,
Archbold, OH 43502

Plaintiffs,

vs.

CENTURYLINK, Inc.
% CT Corporation System, Registered Agent
4400 Easton Commons Way, Suite 125
Columbus, OH 43219

AND

MONGODB, INC.
% Corporation Service Company, Registered Agent
80 State Street
Albany, NY 12207-2543

Defendants.

CASE NO.

JUDGE

MAGISTRATE JUDGE

CLASS ACTION COMPLAINT FOR DAMAGES
(with Jury Demand)

Plaintiffs PATRICIA MASALES and CHRISTOPHER MASALES (collectively, "Plaintiffs") bring this action individually, and on behalf of all others similarly situated, by and through counsel, and against Defendants CENTURYLINK, INC. ("CenturyLink") and MONGODB, INC. ("MongoDB") (collectively, "Defendants"), and hereby allege as follows:

INTRODUCTION

1. CenturyLink is a global technology company "that provides residential, business, and enterprise customers with a variety of products and services, including internet, phone, cable TV, cloud solutions, and security."[1]

2. CenturyLink maintains personally identifiable information ("PII") relative to its customers, including customers' names, email addresses, phone numbers, physical addresses, the contents of their email correspondence, and other account-specific information (*e.g.*, Century Link account numbers, logs of communications with CenturyLink, etc.).[2]

3. MongoDB is an information technology company that develops and offers database services to a variety of users.

4. As of at least November 17, 2018, CenturyLink stored some or all of the PII it maintained in a database created, operated, and controlled by MongoDB (the "Database").[3]

5. On September 15, 2019, security researcher Bob Diachenko ("Diachenko") discovered that the Database "was made publicly available such that no authentication was required to access it" (the "Security Flaw").[4] Although "Diachenko notified CenturyLink" of the Security Flaw that same day, "the database had already been exposed for many months"—approximately 10 months in total.[5] "This would have given malicious parties more than ample time to use the data in various schemes."[6]

---

[1] Comparitech, *CenturyLink Customer Details Exposed Online, 2.8 Million Records Leaked*, available at: https://www.comparitech.com/blog/information-security/centurylink-data-leak/.

[2] *Id*.
[3] *Id*.
[4] *Id*.
[5] *Id*.
[6] *Id*.

6. At the time the Security Flaw was discovered, the Database contained more than 2.8 million records of consumer PII in total.[7]

7. On information and belief, Defendants' failures to adopt, implement, maintain, and enforce proper data security policies and procedures resulted in Plaintiffs' and other similarly situated individuals' PII being improperly disclosed to unauthorized third-parties.

8. Plaintiffs bring this suit on behalf of themselves and a Class of similarly situated individuals against Defendants for Defendants' failure to protect their PII.

PARTIES

9. Plaintiff Patricia Masales is a natural person and resident and citizen of Fulton County, Ohio.

10. Plaintiff Christopher Masales is a natural person and resident and citizen of Fulton County, Ohio.

11. Defendant CenturyLink is a Louisiana corporation with a principal place of business located at 100 CenturyLink Drive, Monroe, Louisiana 71203.

12. Defendant MongoDB is a Delaware corporation with a principal place of business located at 229 West 43rd Street, New York, New York, 10036.

JURISDICTION AND VENUE

13. This Court has personal jurisdiction over Defendants because they regularly conduct business in Ohio and have sufficient minimum contacts in Ohio. Defendants have intentionally availed themselves of this jurisdiction by marketing and selling products and services in Ohio.

[7] *Id.*

14. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because Plaintiffs believe the amount in controversy in this matter exceeds $5,000,000 and because members of the putative Class are from different states than some or all of Defendants. Indeed, according to a recent news article, the Database contained records for at least "hundreds of thousands" of individuals.[8]

15. Venue is proper in this District, pursuant to 28 U.S.C. § 1391 because a substantial portion of the transactions and occurrences relevant to this action took place in this District.

DAMAGES FROM DATA BREACHES

16. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[9]

17. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

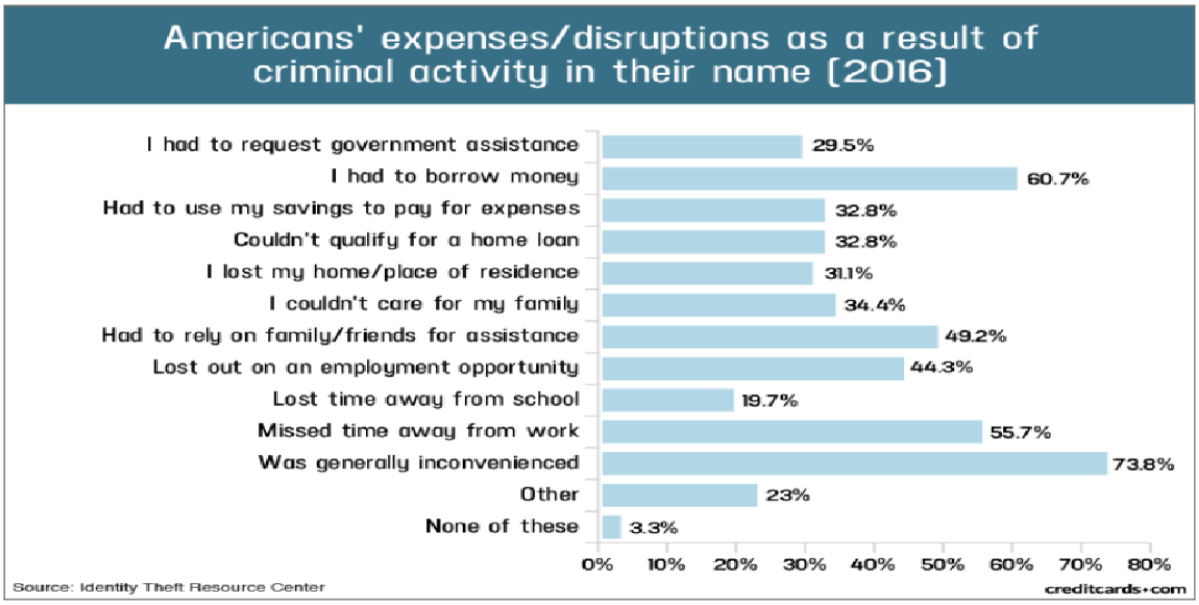
18. Identity thieves can also use stolen PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services in the victim's name, access various other accounts, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

---

[8] *Id*.

[9] U.S. Government Accountability Office, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, p. 2, June 2007, available at: https://www.gao.gov/new.items/d07737.pdf.

19. A study by the Identity Theft Resource Center show the multitude of harms caused by fraudulent use of personal information:[10]



20. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office, 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.

See, GAO Report, p. 29.

21. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. "Consumers sometimes discover their credentials have been stolen only after fraudsters use their

[10] Jason Steele, *Credit Card and ID Theft Statistics*, October 24, 2017, available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

personal medical ID to impersonate them and obtain health services. When unpaid bills are sent on to debt collectors, they track down fraud victims and seek payment."[11]

22. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Defendants' customers are at an increased risk of fraud and identity theft for years into the future.

THE DATA BREACH

23. Plaintiffs and Class members entrusted their PII with CenturyLink in connection with the technology services provided to them by CenturyLink. CenturyLink in turn shared and entrusted Plaintiffs' and Class members' PII with MongoDB through the use of the Database.

24. On information and belief, when CenturyLink contracted with MongoDB for database services, CenturyLink required MongoDB's employees to attend an information privacy course created, developed, and taught by CenturyLink. On information and belief, MongoDB and its employees were also required to sign an agreement that they would comply with CenturyLink's data security procedures. Accordingly, although the Database was operated by MongoDB, CenturyLink exercised significant control and authority as to the security of the Database.

25. As set forth above, although the Database contained sensitive PII, Defendants failed to implement and adopt reasonable procedures to ensure that Plaintiffs' and Class members' PII would be protected from access by malicious third-parties. The Database contained a Security Flaw that permitted anyone to access Plaintiffs' and Class members' PII.

[11] Reuters, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, available at: https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

26. On information and belief, third-parties did, in fact, access and obtain Plaintiffs' and Class members' PII from the Database as a direct result of the Security Flaw.

27. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

28. Plaintiffs and members of the Class have or will suffer actual injury as a direct result of the Security Flaw. In addition to financial fraud and damage to their credit, many victims have or will suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Security Flaw relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Contacting their financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

j. Resetting other accounts that were compromised;

k. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

l. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

29. Plaintiffs and Class members have an interest in ensuring that their personal and financial information, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

30. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have also suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

31. The aforementioned harms to Plaintiffs and Class members was compounded by the fact that, despite becoming aware of the Security Flaw on September 15, 2019, CenturyLink did not inform Plaintiffs and Class members of the Security Flaw until approximately November 19, 2019. This gave malicious third-parties additional time to utilize Plaintiffs' and Class members' PII for nefarious purposes, and deprived Plaintiffs and Class members of the ability to take remedial measures sooner.

FACTS RELEVANT TO PLAINTIFFS

32. On November 19, 2019, CenturyLink sent Plaintiffs an email confirming that Plaintiffs' PII had been stored on the Database and was subject to the Security Flaw.

33. On information and belief, one or more third-parties accessed and stole Plaintiffs' PII stored on the Database as a direct result of the Security Flaw. On information and belief, that third-party (or those third-parties), used Plaintiffs' stolen PII for a variety of malicious purposes. The specific bases for that belief are set forth below.

34. Plaintiffs each have an email account furnished by CenturyLink, and those email accounts are linked to other accounts at various websites. As such, by obtaining access to Plaintiffs' CenturyLink email accounts, third-parties were able to obtain access to Plaintiffs' other online accounts. For example:

a. The login information for Plaintiff Patricia Masales's LifeLock[12] account was changed, such that she is unable to access it;

b. A third-party logged into Plaintiff Patricia Masales's Facebook account by resetting her password via her CenturyLink email account;

c. A third-party logged into Plaintiff Patricia Masales's Amazon account and changed the associated email address to another email address that has no connection to Plaintiff Masales; and

d. Plaintiff Patricia Masales received several other emails stating that she opened various online accounts that she never personally opened.

35. In addition, Plaintiffs have been unable to access their online CenturyLink billing account for several months, and have been unable to pay their CenturyLink bills online.

36. Plaintiffs have also received "phishing" emails which seek to obtain additional PII from Plaintiffs through deceptive means. These "phishing" emails are particularly advanced because they contain personalized information which makes them almost indistinguishable from legitimate emails.

37. All of the foregoing unusual and unauthorized activity relative Plaintiffs' various online accounts has a common denominator: their CenturyLink email and billing accounts. Moreover, Plaintiffs do not use public Wi-Fi and both utilize data protection software on all of their electronic devices, which further supports the conclusion that this unusual and unauthorized activity emanated from the PII stolen from the Database as a result of the Security Flaw.

[12] LifeLock is a service that allows individuals to monitor unusual activity with their PII and helps protect them from identity theft.

38. As a result of this unusual and unauthorized activity, Plaintiffs took and continue to take measures that they otherwise would not have taken to ensure that their identities are not stolen and that her accounts are not compromised. For example, Plaintiff Patricia Masales has been required to place secondary control measures on several of her accounts to ensure that she does not lose access once again. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs have incurred, and will continue to incur, costs and expenses in the form of the time they spent, and will continue to spend, dealing with the theft of her PII.

39. As a direct and proximate result of Defendants' conduct, Plaintiffs have also been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft because their CenturyLink email accounts contain messages with even more sensitive PII (such as credit card numbers, financial information, tax information, etc.).

40. In addition, Plaintiffs have suffered anxiety and emotional distress as a direct and proximate result of Defendants' failures to keep her PII secure.

41. Plaintiffs were further harmed by Defendants' failure to timely inform them of the Security Flaw, as it allowed malicious third-parties to continue to utilize their stolen PII for nefarious means for over a month. Indeed, the login information for Plaintiff Patricia Masales's Facebook and Amazon accounts was changed within the last few days. Plaintiff Patricia Masales could, and would, have taken proactive steps to prevent this authorized access entirely had she been aware of the Security Flaw sooner.

CLASS ALLEGATIONS

42. **Class Definition**: Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23, on behalf of a nationwide class of similarly situated individuals and entities (the "Class"), defined as follows:

> All individuals and entities whose PII was obtained from the Database as a result of the Security Flaw.
>
> Excluded from the Class are: (1) Defendants, Defendants' agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendants or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

43. **Numerosity and Ascertainability**: Upon information and belief, the Class is comprised of hundreds of thousands of individuals and entities,[13] and is so numerous that joinder of all members is impracticable. While the exact number of Class members is presently unknown and can only be ascertained through discovery, Class members can be identified through Defendants' records or by other means.

44. **Commonality and Predominance**: There are several questions of law and fact common to the claims of the Plaintiffs and members of the Class which predominate over any individual issues, including:

a. Whether Defendants adequately protected Plaintiffs' and Class members' PII;

b. Whether Defendants adopted, implemented, and maintained reasonable policies and procedures to prevent the unauthorized access to the Database;

c. Whether Defendants properly trained their employees to prevent the unauthorized access to the Database;

d. Whether Defendants failed to promptly notify their customers of the Database's Security Flaw;

[13] Comparitech, *CenturyLink Customer Details Exposed Online, 2.8 Million Records Leaked*, available at: https://www.comparitech.com/blog/information-security/centurylink-data-leak/ (noting that the Database contained PII for "hundreds of thousands" of individuals).

e. Whether Defendants owed a duty to Plaintiffs and Class members to safeguard and protect their PII;

f. Whether Defendants breached their duty to protect Plaintiffs' and Class members' PII by their failure to adopt, implement, and maintain reasonable policies and procedures to prevent the unauthorized access to the Database; and

g. Whether Defendants are liable for the damages suffered by Plaintiffs and Class members as a result of the theft of their PII, as well as the measure and amount of Plaintiffs' and Class members' damages.

45. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. All claims are based on the same legal and factual issues. Plaintiffs and each of the Class members were customers of CenturyLink, provided their PII to Defendants, entrusted Defendants with their PII, and had their PII accessed and stolen from the Database without authorization. Defendants' conduct was uniform to Plaintiffs and all Class members.

46. **Adequacy of Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the Class, and have retained counsel competent and experienced in complex class actions. Plaintiffs have no interest antagonistic to those of the Class, and Defendants have no defenses unique to Plaintiffs.

47. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiffs' and Class members' claims are manageable.

COUNT I
Negligence

48. Plaintiffs repeat and re-allege the allegations of paragraphs 1-47 with the same force and effect as though fully set forth herein.

49. Defendants knew, or should have known, of the risks inherent in collecting and storing Plaintiffs' and Class members' PII and the importance of adequate security. Defendants were well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

50. Defendants had a common law duty to prevent foreseeable harm to those whose PII they were entrusted. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Defendants to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' PII would not be accessible in an unsecured online Database which was not password-protected.

51. Defendants each had a special relationship with Plaintiffs and Class members. Defendants were entrusted with Plaintiffs' and Class members' PII, and Defendants were in a position to protect that PII from public exposure.

52. Defendants' duties also arose under section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair…practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' PII. Various FTC publications and data security breach orders further form the basis for Defendants' duties.

53. Defendants' duties also arose pursuant to state laws, which require, *inter alia*, companies to implement and maintain reasonable security measures to protect consumers' personal and financial information and promptly notify individuals of any breach. *See e.g.*, Ohio Rev. Code § 1349.19B(2); Del. Code Ann. tit. 6, § 12B-102; N.Y. Gen. Bus. Law § 899-aa; Tex. Bus. & C § 521.053; 815 ILCS 530/10(b).

54. Defendants each had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal and financial information in their possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

55. More specifically, Defendants' duties included, *inter alia*, the duty to:

a. Adopt, implement, and maintain policies, procedures, and security measures for protecting PII, including policies, procedures, and security measures to ensure that PII is not accessible online in unsecured storage servers and are password-protected;

b. Adopt, implement, and maintain reasonable policies and procedures to prevent the sharing of individuals' PII with entities that failed to adopt, implement, and maintain policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

c. Adopt, implement, and maintain reasonable policies and procedures to ensure that they are sharing individuals' PII only with entities that have adopted, implemented, and maintained policies, procedures, and security measures to ensure that the documents are not accessible online in unsecured storage servers and are password-protected;

d. Properly train their employees to protect individuals' PII; and

e. Adopt, implement, and maintain processes to quickly detect data breaches and/or security flaws, and to promptly act on warnings about data breaches and/or security flaws.

56. Defendants breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' PII so that their PII would not come within the possession, access, or control of unauthorized persons.

57. Defendants acted with reckless disregard for the security of Plaintiffs' and Class members' PII because Defendants knew or should have known that their data security practices were not adequate to safeguard the PII that they collected and stored, and because Defendants failed to promptly detect the Security Flaw.

58. As a result of Defendants' conduct, Plaintiffs and Class members have suffered, and will continue to suffer, actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and rectifying unauthorized access to their various other accounts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered, and will continue to suffer, other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

59. Defendants also had an affirmative duty to notify Plaintiffs and Class members in the most expedient time possible the Security Flaw if it was, or is reasonably believed to have been, exploited by an unauthorized person to acquire PII, so that Plaintiff and Class members could take appropriate and timely measures to mitigate damages, protect against adverse consequences, and thwart future incidences of identity theft. *See e.g.*, Ohio Rev. Code § 1349.19B(2); Del. Code Ann. tit. 6, § 12B-102; N.Y. Gen. Bus. Law § 899-aa; Tex. Bus. & C § 521.053; 815 ILCS 530/10(b).

60. Defendants breached their duty to timely inform Plaintiffs and Class members of the Security Flaw because they became aware of the Security Flaw on September 15, 2019, but did not inform Plaintiffs and Class members of the Security Flaw until approximately November 19, 2019.

61. As a result of Defendants' failure to provide timely notification to Plaintiffs and Class members of the Security Flaw, Defendants prevented Plaintiffs and Class members from taking timely and proactive steps to secure their financial data, bank accounts, and other accounts

where their personal and financial information could be used for fraudulent purposes, including identity theft.

COUNT II
Violation of the Consumer Fraud and Deceptive Trade Practices Acts of the Various States and District of Columbia

62. Plaintiffs repeat and re-allege the allegations of paragraphs 1-47 with the same force and effect as though fully set forth herein.

63. Plaintiffs bring this Count individually, and on behalf of the Class for violations of the respective statutory consumer protection laws, as follows:

A. the Alabama Deceptive Trade Practices Act, Ala.Code 1975, § 8–19–1, *et seq.*;

B. the Alaska Unfair Trade Practices and Consumer Protection Act, AS § 45.50.471, *et seq.*;

C. the Arizona Consumer Fraud Act, A.R.S §§ 44-1521, *et seq.*;

D. the Arkansas Deceptive Trade Practices Act, Ark.Code §§ 4-88-101, *et seq.*;

E. the California Unfair Competition Law, Cal.Bus. & Prof. Code §§17200, *et seq*. and 17500 *et seq.*;

F. the California Consumers Legal Remedies Act, Civil Code §§1750, *et seq.*;

G. the Colorado Consumer Protection Act, C.R.S.A. §6-1-101, *et seq.*;

H. the Connecticut Unfair Trade Practices Act, C.G.S.A. § 42-110a, *et seq.*;

I. the Delaware Consumer Fraud Act, 6 Del. C. § 2511, *et seq.*;

J. the D.C. Consumer Protection Procedures Act, DC Code § 28-3901, *et seq.*;

K. the Florida Deceptive and Unfair Trade Practices Act, FSA § 501.201, *et seq.*;

L. the Georgia Fair Business Practices Act, OCGA § 10-1-390, *et seq.*;

M. the Hawaii Unfair Competition Law, H.R.S. § 480-1, *et seq.*;

N. the Idaho Consumer Protection Act, I.C. § 48-601, *et seq.*;

O. the Ohio Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 501/1 *et seq.*;

P. the Indiana Deceptive Consumer Sales Act, IN ST § 24-5-0.5-2, *et seq.*;

Q. The Iowa Private Right of Action for Consumer Frauds Act, Iowa Code Ann. § 714H.1, *et seq.*;

R. the Kansas Consumer Protection Act, K.S.A. § 50-623, *et seq.*;

S. the Kentucky Consumer Protection Act, KRS 367.110, *et seq.*;

T. the Louisiana Unfair Trade Practices and Consumer Protection Law, LSA-R.S. 51:1401, *et seq.*;

U. the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 205-A, *et seq.*;

V. the Maryland Consumer Protection Act, MD Code, Commercial Law, § 13-301, *et seq.*;

W. the Massachusetts Regulation of Business Practices for Consumers Protection Act, M.G.L.A. 93A, *et seq.*;

X. the Michigan Consumer Protection Act, M.C.L.A. 445.901, *et seq.*;

Y. the Minnesota Prevention of Consumer Fraud Act, Minn. Stat. § 325F.68, *et seq.*;

Z. the Mississippi Consumer Protection Act, Miss. Code Ann. § 75-24-1, *et seq.*;

AA. the Missouri Merchandising Practices Act, V.A.M.S. § 407.010, *et seq.*;

BB. the Montana Unfair Trade Practices and Consumer Protection Act of 1973, Mont. Code Ann. § 30-14-101, *et seq.*;

CC. the Nebraska Consumer Protection Act, Neb.Rev.St. §§ 59-1601, *et seq.*;

DD. the Nevada Deceptive Trade Practices Act, N.R.S. 41.600, *et seq.*;

EE. the New Hampshire Regulation of Business Practices for Consumer Protection, N.H.Rev.Stat. § 358-A:1, *et seq.*;

FF. the New Jersey Consumer Fraud Act, N.J.S.A. 56:8, *et seq.*;

GG. the New Mexico Unfair Practices Act, N.M.S.A. §§ 57-12-1, *et seq.*;

HH. the New York Consumer Protection from Deceptive Acts and Practices, N.Y. GBL (McKinney) § 349, *et seq.*;

II. the North Carolina Unfair and Deceptive Trade Practices Act, N.C. Gen Stat. § 75-1.1, *et seq.*;

JJ. the North Dakota Consumer Fraud Act, N.D. Cent.Code Chapter 51-15, *et seq.*;

KK. the Ohio Consumer Sales Practices Act, R.C. 1345.01, *et seq.*;

LL. the Oklahoma Consumer Protection Act, 15 O.S.2001, §§ 751, *et seq.*;

MM. the Oregon Unlawful Trade Practices Act, ORS 646.605, *et seq.*;

NN. the Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. § 201-1, *et seq.*;

OO. the Rhode Island Deceptive Trade Practices Act, G.L.1956 § 6-13.1-5.2(B), *et seq.*;

PP. the South Carolina Unfair Trade Practices Act, SC Code 1976, §§ 39-5-10, *et seq.*;

QQ. the South Dakota Deceptive Trade Practices and Consumer Protection Act, SDCL § 37-24-1, *et seq.*;

RR. the Tennessee Consumer Protection Act, T.C.A. § 47-18-101, *et seq.*;

SS. the Texas Deceptive Trade Practices-Consumer Protection Act, V.T.C.A., Bus. & C. § 17.41, *et seq.*;

TT. the Utah Consumer Sales Practices Act, UT ST § 13-11-1, *et seq.*;

UU. the Vermont Consumer Fraud Act, 9 V.S.A. § 2451, *et seq.*;

VV. the Virginia Consumer Protection Act of 1977, VA ST § 59.1-196, *et seq.*;

WW. the Washington Consumer Protection Act, RCWA 19.86.010, *et seq.*;

XX. the West Virginia Consumer Credit And Protection Act, W.Va.Code § 46A-1-101, *et seq.*;

YY. the Wisconsin Deceptive Trade Practices Act, WIS.STAT. § 100, *et seq.*; and

ZZ. the Wyoming Consumer Protection Act, WY ST § 40-12-101, *et seq.*

64. Defendants engaged in unfair and deceptive acts or practices when they accepted and stored Plaintiffs' and Class members' PII and then failed to adopt, implement, and maintain reasonable measures to protect that PII.

65. Defendants represented to Plaintiffs and Class members that their PII would be safeguarded from access by unauthorized individuals, and that they would inform Plaintiffs and Class members of any threats to the security of their PII.

66. For example, on its website, CenturyLink represents that it "takes immense precautions in monitoring, preventing, and identifying fraudulent behavior related to its website,"[14] states that "when malicious activity is detected on your account, we provide web and email (when available) notifications for your protection,"[15] and markets a variety of data security products.[16] CenturyLink also states that when it shares PII with other companies, it "require[s] these companies to use our information only for the purposes we specify and to keep it safe and confidential." In addition, CenturyLink's privacy policy states that: "Only CenturyLink employees, agents, service providers and other businesses we work and share information with and who have a legitimate business purpose are authorized to access customer information. This access is strictly defined (often involving password controlled access and other security controls) and subject to policies and contracts requiring confidential treatment of the information…We use secure technologies to transfer sensitive information and comply with a variety of industry standards, and federal and state laws regarding the protection of customer information."[17]

---

[14] CenturyLink, *Online Security*, available at: https://www.centurylink.com/aboutus/legal/online-security.html.

[15] CenturyLink, *CenturyLink Consumer Internet Protection Program*, available at: https://www.centurylink.com/home/support/internetprotection/.

[16] *See,e.g.*, CenturyLink, *Enhanced Cybersecurity Services*, available at: https://www.centurylink.com/business/resources/product-finder.html#security; CenturyLink, *Cloud Security*, available at: https://www.centurylink.com/business/security/cloud.html; CenturyLink, *Email Security*, available at: https://www.centurylink.com/business/security/email-security.html.

[17] CenturyLink, *Complete Privacy Policy*, available at: https://www.centurylink.com/aboutus/legal/privacy-

CenturyLink's privacy policy also states that "We have security measures in place to protect against [unauthorized] access."[18]

67. Similarly, MongoDB's website states that it "has been independently audited and confirmed to meet compliance standards for data security,"[19] is "dedicated to making every effort to protect customer data, including continually improving security processes and controls," [20] and is "committed to delivering the highest levels of standards conformance and regulatory compliance as part of our ongoing mission to address the most demanding security and privacy requirements of our customers."[21] MongoDB's website also states that it is "committed to protecting the privacy of your data stored in our products and services," and that "access is restricted tightly and monitored using both logical controls and management processes."[22] Finally, MongoDB's privacy policy states as follows: "Once we have received your information, we use a variety of industry-standard security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. We also require you to enter a password to access your account information."[23]

68. For the reasons set forth above, the foregoing representations were false.

69. Defendants intended for Plaintiffs and the members of the Class to rely upon their misrepresentations and omissions, and Plaintiffs and Class members did, in fact, rely upon these misrepresentations and omissions.

70. Had Plaintiffs and Class members known that Defendants did not have adequate measures in place to protect their PII, they would not have entrusted their PII to Defendants

---

policy/privacy-policy-complete.html.

[18] *Id*.

[19] MongoDB, *Security*, available at: https://www.mongodb.com/cloud/atlas/security.

[20] MongoDB, *Trust Center*, available at: https://www.mongodb.com/cloud/trust.

[21] MongoDB, *Trust Center*, available at: https://www.mongodb.com/cloud/trust.

[22] MongoDB, *Trust Center*, available at: https://www.mongodb.com/cloud/trust.

[23] MongoDB, *Privacy Policy*, available at: https://www.mongodb.com/legal/privacy-policy.

and/or would have required Defendants to adopt, implement, and maintain adequate security measures, including measures to ensure the information would not be provided to third parties that did not have adequate measures in place, before providing their PII.

71. The above-described deceptive and unfair acts and practices were used or employed in the conduct of trade or commerce.

72. The above-described deceptive and unfair acts offend public policy and cause substantial injury to consumers.

73. Defendants' conduct implicates consumer protection concerns as their data security practices affect the public generally.

74. As a result of Defendants' conduct, Plaintiffs and Class members have suffered, and will continue to suffer, actual damages including, but not limited to, expenses and/or time spent on credit monitoring; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and rectifying unauthorized access to their various other accounts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered, and will continue to suffer, other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

75. Plaintiffs and Class members have suffered damages as a direct and proximate result of Defendants' unfair and unconscionable commercial practices. These substantial injuries outweigh any benefit to consumers or competition that may result from Defendants' unfair practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs PATRICIA MASALES and CHRISTOPHER MASALES, individually, and on behalf of all others similarly situated, pray for an Order as follows:

A. Finding that this action satisfies the prerequisites for maintenance as a class action and certifying the Class defined herein;

B. Designating Plaintiffs as representatives of the Class, and their undersigned counsel as Class Counsel;

C. Entering judgment in favor of Plaintiffs and the Class, and against Defendants;

D. Awarding Plaintiffs and the Class actual damages, punitive damages, and all other forms of available relief;

E. Entering an injunction requiring Defendants to adopt, implement, and maintain adequate security measures to protect Plaintiffs' and Class members' PII;

F. Awarding Plaintiffs' Counsel their attorney's fees and costs, including interest thereon, as allowed or required by law; and

G. Granting all such further and other relief as the Court deems just and appropriate.

JURY DEMAND

Plaintiffs demand a trial by jury on all counts so triable.

Respectfully Submitted,

/s/ Marc E. Dann
Marc E. Dann (0039425)
Brian D. Flick (0081605)
DANNLAW
P.O. Box. 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Matthew C. De Re (*pro hac vice* anticipated)
matt@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com

Counsel for Plaintiffs and the putative Class