Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4787
Facsimile: (916) 924-1829
gharoutunian@justice4you.com
bjack@justice4you.com

Kaleigh N. Boyd (WSBA No. 52684)
TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Telephone: (206) 682-5600
Facsimile: (206) 682-2992
kboyd@tousley.com

Attorneys for Plaintiffs and the Class

Per local Rule, This case is assigned to Judge Treat, Charles S, for all purposes.

SUMMONS ISSUED

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF CONTRA COSTA

MIRIAM ELIZONDO, individually and on behalf of herself and all others similarly situated,

Plaintiff,

v.

UMPQUA BANK,

Defendant.

Case No. C23-02123

CLASS ACTION COMPLAINT FOR:
(1) NEGLIGENCE;
(2) BREACH OF THIRD-PARTY BENEFICIARY CONTRACT;
(3) VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE § 17200, *ET SEQ.*) (UNLAWFUL BUSINESS PRACTICES);
(4) VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW (CAL. BUS. & PROF. CODE § 17200, *ET SEQ.*) (UNFAIR BUSINESS PRACTICES)

DEMAND FOR JURY TRIAL

Plaintiff Miriam Elizondo ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Umpqua Bank ("Defendant" or "Umpqua"), and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive information that Plaintiff and Class Members, as customers of Umpqua, entrusted to it, including, without limitation, their names and Social Security numbers (collectively, "personally identifiable information" or "PII").[1]

2. Defendant is community bank based in Oregon that recently merged with Columbia Bank in Washington.

3. Plaintiff and Class Members are current and former customers of Umpqua.

4. As a condition of receiving its services, Umpqua requires that its customers, including Plaintiff and Class Members, entrust it with highly sensitive personally identifiable information ("PII"), including but not limited to their names and Social Security numbers.

5. Plaintiff and Class Members provided their PII to Umpqua with the reasonable expectation and on the mutual understanding that Umpqua would comply with its obligations to keep that information confidential and secure from unauthorized access.

6. Umpqua derives a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without it, Umpqua could not perform its services.

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

7. Umpqua had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its vendors and affiliates for their own cybersecurity. Umpqua has a legal duty to keep consumer's PII safe and confidential.

8. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Umpqua assumed legal and equitable duties to ensure the protection of that PII, and it knew or should have known that it was thus responsible for protecting Plaintiff's and Class Members' PII from disclosure.

9. On or about August 11, 2023, Umpqua began sending Plaintiff and other Class Members notice (the "Notice Letter") informing them that their PII had been exposed as a result of a breach of a tool used by one of Umpqua's vendors to store and transfer PII (the "Data Breach").[2]

10. Noticeably absent from the Notice Letter are details of the root cause of the Data Breach, the vulnerabilities that were exploited, and the remedial measures that Umpqua undertook to ensure such a breach does not happen again. To date, these critical facts have not been explained or clarified to Plaintiff or the Class Members, who have a vested interest in ensuring that their PII remains protected.

11. In fact, the attacker accessed and acquired files that Umpqua shared with its vendor containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers.

12. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware and software containing protected PII using reasonable and

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7589df9f-75b6-417f-afa0-68eeec2e7de9.shtml (last accessed 8/22/2023)

effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to, among other things, negligence and violates federal and state statutes.

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their private information; and (v) the continued and certainly increased risk to their PII a, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded; failing to take available steps to prevent an unauthorized disclosure of data; and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Miriam Elizondo

15. Plaintiff Miriam Elizondo is a citizen of California and resides in Humboldt County. Ms. Elizondo is a customer of Umpqua Bank. She received an email informing her of the data breach and informing her she would be receiving a *Notice of Data Breach* letter shortly on or about August 15, 2023, and she received an undated *Notice of Data* Breach letter, on or about that

date, which specially identified that her personal information, including her name and Social Security number were exposed by the Data Breach.

Defendant Umpqua Bank

16. Defendant Umpqua Bank is an Oregon state-chartered bank with its principal place of business at 5005 Meadows Road, Suite 400, Lake Oswego, Oregon.

III. JURISDICTION AND VENUE

17. This Court has jurisdiction over this matter pursuant to the California Constitution, Article VI, § 10 and California Code of Civil Procedure ("CCP") § 410.10, because Defendant transacted business and committed the acts alleged in California. The amount in controversy exceeds the jurisdictional minimum of this Court.

18. This Court has personal jurisdiction over Defendant because it regularly conducts business in California, including in this County, and because its conduct with respect to Plaintiff, including its collection of Plaintiff's PII and the duties it assumed with respect to Plaintiff, occurred in this County.

19. Venue is appropriate in Contra Costa County because Defendant did and is doing substantial business in Contra Costa County, including gathering the PII of Class Members from Defendant's operations in Contra Costa County.

IV. FACTUAL ALLEGATIONS

The Data Breach

20. As outlined above, Umpqua admitted that its vendor was the subject of a massive data breach that affected millions of its customers. Between May 29 to May 30, 2023, unauthorized third-party cybercriminals exploited a vulnerability in the file transfer protocol software Umpqua's vendor used to store and transfer Umpqua's customers' data.[3]

[3] *Id.*

21. The customer PII the hackers accessed include names and Social Security numbers.[4]

22. Umpqua had obligations to Plaintiff and to Class Members to safeguard their PII and to protect that PII from unauthorized access and disclosure, including by ensuring that its vendors would protect that PII. Indeed, Plaintiff and Class Members provided their PII to Umpqua with the reasonable expectation and mutual understanding that Umpqua, and anyone Umpqua contracted with, would comply with its obligations to keep such information confidential and secure from unauthorized access. Umpqua's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies before the Data Breach.

23. Umpqua also promises to keep the PII it collects secure, even when it provides that PII to third parties. In its Privacy Policy, Umpqua promises that it "use[s] reasonable physical, electronic, and procedural safeguards that comply with federal standards to protect and limit access to personal information. This includes device safeguards and secured files and buildings."[5]

24. It also promises that "We protect your personal information commensurate with its degree of sensitivity."[6]

25. As a result of the Data Breach, Umpqua is urging affected consumers to monitor their accounts for suspicious activity and to safeguard themselves against possible fraud.[7] Furthermore, numerous data security experts are also suggesting that affected consumers take steps to protect their identities.

Plaintiff Expected Umpqua and its Vendors to Keep Her Information Secure

---

[4] *Id.*

[5] *See* Privacy at Columbia Banking Systems, Inc., *available at* https://www.umpquabank.com/privacy/ (last accessed 8/22/2023)

[6] *Id.*

[7] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/7589df9f-75b6-417f-afa0-68eeec2e7de9.shtml. (last accessed 8/22/2023)

26. Plaintiff Miriam Elizondo is a customer of Umpqua Bank.

27. As a condition of receiving products and services from Umpqua, Ms. Elizondo provided her PII to Umpqua, which Umpqua then gave to one of its vendors, who stored and maintained it.

28. Ms. Elizondo places significant value on the security of her PII, especially when receiving banking services. She entrusted her sensitive PII to Umpqua with the understanding that Umpqua and those with whom Umpqua contracted would keep her information secure and employ reasonable and adequate security measures to ensure that it would not be compromised.

29. Additionally, Plaintiff is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

30. Ms. Elizondo received an undated letter on or around August 15, 2023, informing her that her PII was compromised in the Data Breach.

31. As a result of Umpqua's exposure of Ms. Elizondo's PII, she will have to spend hours attempting to mitigate the affects of the Data Breach, including monitoring financial and other important accounts for fraudulent activity.

32. Given the highly sensitive nature of the information that was compromised, Ms. Elizondo has already suffered injury and remains at a substantial and imminent risk of future harm. In fact, because her Social Security number is impacted, Ms. Elizondo faces this risk for her lifetime. She has experienced anxiety concerning whether the bad actors that accessed and exfiltrated her PII will use it to commit identity theft or other financial crimes.

33. In addition, Ms. Elizondo has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Umpqua's possession, is protected, and safeguarded from future breaches.

FTC Security Guidelines Concerning PII

34. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

35. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

36. In 2016, the FTC provided updated security guidelines in a publication titled Protecting Personal Information: A Guide for Business. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention to the security of web applications—the software used to inform visitors to a company's website and to retrieve information from the visitors.

37. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the industry; and verify that third parties with access to sensitive information use reasonable security measures.

38. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

39. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

40. When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers'

privacy rights or misled them by failing to maintain security for sensitive consumer information or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.[8]

41. Umpqua was aware or should have been aware of its obligations to protect its clients' customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, Umpqua violated its obligations under Section 5 of the FTC Act.

Umpqua Was on Notice of Data Threats and the Inadequacy of Its Vendor's Data Security

42. Umpqua was on notice that companies maintaining large amounts of PII during their regular course of business are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information, such as the type of data at issue in this case.

43. At all relevant times, Umpqua knew, or should have known, that the PII that it collected was a target for malicious actors. Despite such knowledge, and well-publicized cyberattacks on similar companies, Umpqua failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class Members' PII from cyber-attacks that Umpqua should have anticipated and guarded against.

44. It is well known among companies that store PII that sensitive information—such as the Social Security numbers accessed in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[9]

---

[8] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last accessed 8/22/2023)

[9] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies*

45. In light of recent high profile data breaches, including Microsoft (250 million records, December 2019), T-Mobile (110 million records, August 2021), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Umpqua knew or should have known that its electronic records would be targeted by cybercriminals.

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

The Data Breach Harmed Plaintiff and Class Members

47. Plaintiff and Class Members have suffered and will continue to suffer harm because of the Data Breach.

48. Plaintiff and Class Members face a present and imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach for their respective lifetimes. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and PHI—thereby risking prosecution by listing it for sale on the dark web—if the PII and PHI was not valuable to malicious actors.

49. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

50. Malicious actors use PII and PHI to gain access to Class Members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can

---

recently, your data may have been stolen, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1 (last accessed 8/22/2023)

harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

51. Consumers are injured every time their data is stolen and placed on the dark web, even if they have been victims of previous data breaches. Not only is the likelihood of identity theft increased, but the dark web is not like Google or eBay. It is comprised of multiple discrete repositories of stolen information. Each data breach puts victims at risk of having their information uploaded to different dark web databases and viewed and used by different criminal actors.

52. Umpqua issued misleading public statements about the Data Breach, including its data breach notification letters,[10] in which it attempts to downplay the seriousness of the Data Breach by stating that there is "no evidence at this time that your personal information has been used in an unauthorized way."

53. Umpqua has also vaguely stated that it "immediately worked with our vendor to ensure that they had resolved the vulnerability to keep our customer information safe following the incident and moving forward" without giving any details of what steps, exactly, it took. Plaintiff and Class Members are thus left to guess whether Umpqua has, in fact, addressed the root causes of the Data Breach to ensure that Plaintiff and Class Members' PII cannot be accessed again.

54. Umpqua's intentionally misleading public statements ignore the serious harm its security flaws caused to the Class. Even worse, those statements could convince Class Members that they do not need to take steps to protect themselves.

55. The data security community agrees that the PII compromised in the Data Breach greatly increases Class Members' risk of identity theft and fraud.

56. As Justin Fier, senior vice president for AI security company Darktrace, observed following a recent data breach at T-Mobile, "[t]here are dozens of ways that the information that

[10] *Available at* https://apps.web.maine.gov/online/aeviewer/ME/40/7589df9f-75b6-417f-afa0-68eeec2e7de9.shtml (last accessed 8/22/2023)

was stolen could be weaponized." He added that such a massive treasure trove of consumer profiles could be of use to everyone from nation-state hackers to criminal syndicates.[11]

57. Criminals can use the PII that Umpqua lost to target Class Members for imposter scams, a type of fraud initiated by a person who pretends to be someone the victim can trust in order to steal sensitive data or money.[12]

58. The PII accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again.

59. Malicious actors can also use Class Members' PII to open new financial accounts, open new utility accounts, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

60. As established above, the PII accessed in the Data Breach is also very valuable to Umpqua. Umpqua collects, retains, and uses this information to increase its profits. Umpqua's customers value the privacy of this information and expect Umpqua to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Umpqua, provided their PII to Umpqua, and/or paid the same prices for Umpqua's goods and services had they known Umpqua did not implement reasonable security measures to protect PII. Umpqua states that it "develop[s] trust and build[s] mutually beneficial relationships by respecting your privacy and your choices."[13] Customers expect that the payments they make to Umpqua incorporate the costs to implement reasonable security measures to protect customers' PII as part of protecting their PII and respecting their privacy.

61. Indeed, "[f]irms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[14] American companies are estimated to have spent over $19 billion on

[11] https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-un-carrier-un-safe/.

[12] *See* https://consumer.ftc.gov/features/imposter-scams.

[13] *See* https://www.umpquabank.com/privacy/.

acquiring personal data of consumers in 2018.[15] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" or the "dark web" for many years.

62. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated, and it can become more valuable to thieves and more damaging to victims.

63. The PII accessed in the Data Breach is also very valuable to Plaintiff and Class Members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (e.g., sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiff and Class Members' PII has been compromised and lost significant value.

64. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

[14] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD DIGITAL ECONOMY PAPERS, No. 220, Apr. 2, 2013, https://doi.org/10.1787/5k486qtxldmq-en. (Last accessed 8/22/2023)

[15] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/. (Last accessed 8/22/2023)

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[16]

65. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

66. Due to the immutable nature of the personal information impacted here, Plaintiff and Class Members will face a risk of injury due to the Data Breach for their respective lifetimes. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiff and Class Members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

67. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud.

68. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims experienced negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

[16] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RES. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1. (Last accessed 8/22/2023)

69. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[17]

70. Plaintiff and Class Members have failed to receive the value of the Umpqua services for which their insurance companies paid.

Defendant Failed to Take Reasonable Steps to Protect its Customers' PII

71. Umpqua requires its customers to provide a significant amount of highly personal and confidential PII to purchase its services. Umpqua collects, stores, and uses this data to maximize profits while failing to encrypt or protect it properly.

72. Umpqua has legal duties to protect its customers' PII by implementing reasonable security features. This duty is further defined by federal and state guidelines and laws, including the FTC Act, as well as industry norms.

73. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiff's and Class Members' PII was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiff and Class Members were harmed.

74. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members and ensuring that its vendor did so as well.

75. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

76. Experts have identified several best practices that business like Umpqua should implement at a minimum, including, but not limited to: educating all employees; requiring strong

[17] *See* https://www.gao.gov/assets/gao-07-737.pdf. (Last accessed 8/22/2023)

passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

78. When using a file transfer protocol, moreover, best cybersecurity practices include not storing data or information longer than necessary to accomplish the transfer. By storing Plaintiff's and Class Members' PII in its file transfer protocol longer than was necessary to accomplish the transfer, Umpqua's vendor—for whom Umpqua was responsible—left Plaintiff's and Class Members' PII vulnerable to access and theft, which is what ultimately happened.

79. The Data Breach was a reasonably foreseeable consequence of Defendant's failure to ensure that its vendors used adequate security systems. Umpqua certainly has the resources to ensure that its vendors implement reasonable security systems to prevent or limit damage from data breaches. Even so, Umpqua failed to properly invest in that data security. Had Umpqua ensured that its vendors implemented reasonable data security systems and procedures (i.e., followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from accessing its customers' PII.

80. Umpqua's failure to ensure that its vendors implemented reasonable security systems has caused Plaintiff and Class Members to suffer and continue to suffer harm that adversely impact Plaintiff and Class Members economically, emotionally, and/or socially. As discussed above, Plaintiff and Class Members now face a substantial, imminent, and ongoing threat of identity theft, scams, and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores and diligently

sift out phishing communications to limit potential adverse effects of the Data Breach, regardless of whether any Class Member ultimately falls victim to identity theft.

81. In sum, Plaintiff and Class Members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) diminution in value of their PII; (iv) the certain, ongoing, and imminent threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (v) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; and/or (vi) nominal damages.

82. Even though Umpqua has decided to offer free credit monitoring for two years to affected individuals, this is insufficient to protect Plaintiff and Class Members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiff and the Classes significant time and effort.

83. Plaintiff and Class Members therefore have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages) that protects them from these long-term threats. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

84. Concurrently with the filing of this Complaint, Plaintiff is providing Umpqua with written notice of its breach of its Privacy Policy, which constitutes part of its contract with Plaintiff and Umpqua's customers. If Umpqua does not timely rectify its data security practices in line with Plaintiff's notice, Plaintiff will amend this Complaint to include an action for Breach of Contract against Defendant.

V. CLASS ACTION ALLEGATIONS

85. Plaintiff brings this action on behalf of herself and all others similarly situated pursuant to Code of Civil Procedure § 382, Civil Code § 1781, and other applicable law as representative of the Classes defined as follows:

The Nationwide Class: All U.S. residents whose data was accessed in the Data Breach.

The California Subclass: All California residents whose data was accessed in the Data Breach.

86. Specifically excluded from the Classes are Defendant; its parents, subsidiaries, affiliates, officers and directors; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Classes are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

87. Class Identity: The members of the Classes are readily identifiable and ascertainable. Defendant and/or its affiliates, among others, possess the information to identify and contact Class Members.

88. Numerosity: The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Nationwide Class of approximately 429,000 individuals whose data was compromised in the Data Breach, and the California Class consists of thousands of customers whose data was compromised in the Data Breach.

89. Typicality: Plaintiff's claims are typical of the claims of the members of the classes because all Class Members had their PII accessed in the Data Breach and were harmed as a result.

90. Adequacy: Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff has no interest antagonistic to those of the classes and is aligned with Class Members' interests because Plaintiff was subject to the same Data Breach as Class Members and faces similar threats due to the Data Breach as Class Members. Plaintiff has also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes.

///

91. Commonality and Predominance: There are questions of law and fact common to the Classes. These common questions predominate over any questions affecting only individual Class Members. The common questions of law and fact include, without limitation:

92. Whether Defendant owed Plaintiff and Class Members a duty to implement and maintain reasonable security procedures and practices to protect their personal information, and to ensure that its vendors did so as well;

93. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiff's and Class Members' PII;

94. Whether Defendant breached its duty to implement reasonable security systems to protect Plaintiff's and Class Members' PII, and to ensure that its vendors did so as well;

95. Whether Defendant breached its contractual obligations to its customers to protect Plaintiff's and Class Members' PII;

96. Whether Plaintiff and Class Members were intended third party beneficiaries of Defendant's contract with its vendor;

97. Whether Defendant's breach of its duty to implement reasonable security systems, and its duty to ensure that its vendors did the same, directly and/or proximately caused damages to Plaintiff and Class Members;

98. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

99. When Defendant learned of the Data Breach and whether its response was adequate;

100. Whether Plaintiff and other Class Members are entitled to credit monitoring and other injunctive relief; and,

101. Whether Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

102. Defendant has engaged in a common course of conduct, and Class Members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and

practices to protect customers' PII and to ensure that the vendors to whom it provided Plaintiff's and Class Members' PII did the same.

103. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all Class Members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members and risk inconsistent treatment of claims arising from the same set of facts and occurrences.

104. Plaintiff knows of no difficulty likely to be encountered in the maintenance of this action as a class action under Federal Rule of Civil Procedure 23.

CLAIMS FOR RELIEF

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Class)

105. Plaintiff repeats and realleges every allegation set forth in the preceding paragraphs.

106. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendant breached its duty of care by failing to ensure that the third parties to whom it provided Plaintiff's and Class Members' PII implement reasonable security procedures and practices to protect that PII. Among other things, Defendant failed to ensure that third party vendors: (i) implemented security systems and practices consistent with federal and state laws and guidelines; and (ii) implemented security systems and practices consistent with industry norms.

107. Defendant knew or should have known that Plaintiff's and Class Members' PII was highly sought after by cyber criminals and that Plaintiff and Class Members would suffer significant harm if their PII was compromised by hackers.

108. Defendant also knew or should have known that timely detection and disclosure of the Data Breach was required and necessary to allow Plaintiff and Class Members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions, and cancelling or monitoring government issued.

109. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff and Class Members entrusted Defendant with several pieces of Plaintiff's and Class Members' PII so that Defendant would provide services to them. Defendant's customers were required to provide this PII when purchasing or attempting to purchase Defendant's services. Plaintiff and Class Members were led to believe Defendant would take reasonable precautions to protect their PII and would timely inform them if their PII was compromised, which Defendant failed to do.

110. The harm that Plaintiff and Class Members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to ensure that the third parties to whom it provided PII enacted reasonable security procedures and practices, and Plaintiff and Class Members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII accessed in the Data Breach is precisely the type of information that cyber criminals seek and use to commit cyber crimes.

111. But-for Defendant's breach of its duty of care, the Data Breach would not have occurred and Plaintiff's and Class Members' PII would not have been accessed by an unauthorized and malicious party.

112. As a direct and proximate result of the Defendant's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Plaintiff and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, among other things, (1) a present and imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (5) deprivation of the value of their Private

Information, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

COUNT II
Breach of Third Party Beneficiary Contract
(On Behalf of Plaintiff and the Nationwide Class or Alternatively the California Class)

113. Plaintiff incorporates by reference the foregoing allegations of fact as if fully set forth herein.

114. Defendant entered into a written contracts with its vendor to provide certain services for which Defendant's vendor required Plaintiff's and Class Members' PII.

115. In exchange, on information and belief, Defendant and its vendor agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

116. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and its vendor.

117. Defendant and/or its vendor breached the contract it entered into by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's PII from unauthorized disclosure to third parties, (iii) failing to perform due diligence and to verify, audit, or monitor the integrity of third party networks on which it shared PII, and (iv) failing to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

118. Plaintiff and Class Members were harmed by Defendant's breach of its contracts with its vendor, its vendor's breach of its contract with Defendant, or both, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

COUNT III
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unlawful Business Practices
(On Behalf of Plaintiff and the California Class)

119. Plaintiff and the California Class re-allege and incorporate by reference herein all of the foregoing allegations as though fully set forth herein.

120. Defendant has violated Cal. Bus. & Prof. Code § 17200, *et seq*., by engaging in unlawful business acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200.

121. Actions for relief may be brought "by a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff is a "person" as defined by Cal. Bus. & Prof. Code § 17201 and has lost money or property as a result of the unfair competition.

122. Defendant engaged in unlawful acts and practices with respect to the services it provided to the California Class by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiff's and the California Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and the California Class Members' PII in an unsecure environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods of safeguarding the PII of Plaintiffs and the California Class.

123. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff and the California Class were injured and lost money or property, including but not limited to the money Defendant received for the services provided, the loss of Plaintiff's and the California Class's legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

124. Defendant knew or should have known that Defendant's data security practices and the data security practices of its vendor were inadequate to safeguard Plaintiff's and the California Class Members' PII and that the risk of a data breach or theft was highly likely, especially given

Defendant's inability to adhere to basic encryption standards and data disposal methodologies. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of California Class Members.

125. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiff and the California Class of money or property that Defendant may have acquired by means of Defendant's unlawful and unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unlawful business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IV
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*. – Unfair Business Practices
(On Behalf of Plaintiff and the California Class)

126. Plaintiff and the California Class re-allege and incorporate by reference herein all of the foregoing allegations as though fully set forth herein.

127. Defendant has violated Cal. Bus. & Prof. Code § 17200, *et seq*. by engaging in unfair business acts and practices that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200.

128. Actions for relief may be brought "by a person who has suffered injury in fact and has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204. Plaintiff is a "person" as defined by Cal. Bus. & Prof. Code § 17201 and has lost money or property as a result of the unfair competition.

129. Defendant engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein, by soliciting and collecting Plaintiff's and the California Class Members' PII with knowledge that the information would not be adequately protected, and by storing Plaintiff's and the California Class Members' PII in an unsecure electronic environment or allowing it to be stored there. These unfair acts and practices were

immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and the California Class. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the California Class outweighed their utility, if any.

130. As a direct and proximate result of Defendant's acts of unfair practices, Plaintiff and the California Class were injured and lost money or property, including but not limited to the price Plaintiff and the California Class paid to Defendant for the services it provided, the loss of Plaintiff's and the California Class Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

131. Defendant knew or should have known that Defendant's data security practices and the data security practices of its vendor were inadequate to safeguard Plaintiff's and the California Class Members' PII and that the risk of a data breach or theft was highly likely, including Defendant's failure to properly encrypt files containing sensitive PII. Defendant's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the California Class.

132. Plaintiff and the California Class seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the California Class of money or property that the Defendant may have acquired by means of Defendant's unfair business practices, restitutionary disgorgement of all profits accruing to Defendant because of Defendant's unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the California Class, and appointing Plaintiff and her Counsel to represent each such Class;

B. That the Court award compensatory, statutory, and exemplary damages;

C. In the alternative, that the Court award nominal damages as permitted by law;

D. That the Court award injunctive or other equitable relief that directs Defendant to provide Plaintiff and the Classes with free identity theft protection and credit monitoring for their respective lifetimes, and to ensure that its vendors implement reasonable security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;

E. That the Court award reasonable costs and expenses incurred in prosecuting this action, including attorneys' fees and expert fees;

F. For pre- and post-judgment interest on all amounts awarded; and

G. Such other relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

DATED: August 24, 2023

Respectfully submitted,

CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION

By: */s/ Gregory Haroutunian*
Gregory Haroutunian, Esq.
Attorneys for Plaintiffs and the Class

ClassAction.org
