M. Anderson Berry (SBN 262879)
Gregory Haroutunian (SBN 330263)
Brandon P. Jack (SBN 325584)
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SOPHIE JANI, individually and on behalf of all others similarly situated, Plaintiff, vs. PATELCO CREDIT UNION, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Sophie Jani, by and through her counsel, brings this Class Action Complaint against Defendant Patelco Credit Union, individually and on behalf of all others similarly situated, and allege, 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. NATURE OF THE ACTION

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 Patelco, entrusted to it, including, without limitation, their names and Social Security numbers (collectively, "personally identifiable information" or "PII").

2. Defendant is a full-service, not-for-profit financial cooperative based in California.[1]

3. Plaintiff and Class Members are current and former customers of Patelco, and family members of current and former customers of Patelco.

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

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

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

7. Patelco 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. Patelco 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, Patelco 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.

[1] *See* https://www.patelco.org/about-patelco/who-we-are/ (last visited October 2, 2023).

9. On or about September 20, 2023, Patelco began sending Plaintiff and other Class Members a Notice of Data Breach (the "Notice Letter") informing them that their PII had been exposed as a result of a breach of a tool used by one of Patelco's vendors to store and transfer PII (the "Data Breach").

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 Patelco 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 Patelco shared with its vendor containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers.

12. Plaintiff brings 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 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

15. Plaintiff Sophie Jani is, and at all times relevant, has been a citizen of Oakland, California. Plaintiff Jani has no intention of moving to a different state in the immediate future. Plaintiff Jani, and her minor twelve (12) year old daughter, each received a Notice of Data Breach letter from Defendant on or around September 20, 2023, regarding the Data Breach.

16. On or about October 2, 2023, pursuant to § 1798.150(b) of the CCPA, Plaintiff Jani separately provided written notice to Defendant identifying the specific provisions of this title she alleges it has violated. If within 30 days of Plaintiff's written notice to Defendant it fails to "actually cure" its violations of Cal. Civ. Code § 1798.150(a) and provide "an express written statement that the violations have been cured and that no further violations shall occur," Plaintiff will amend this complaint to also seek the greater of statutory damages in an amount no less than one hundred dollars ($100) and up to seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater, on behalf of the California Subclass. *See* Cal. Civ. Code § 1798.150(b).

17. Defendant Patelco Credit Union is a California-based credit union with its principal place of business at 3 Park Plaza, Dublin, California 94568.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the State of California, and have different citizenship from Defendant. Indeed, the Office of the Maine Attorney General has confirmed that there are at least 31 Maine residents who were affected by the Data Breach.[2] Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

19. This Court has jurisdiction over Defendant because it operates in this District, and because it has its principal place of business and headquarters in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District, Defendant has harmed Class Members residing in this District, and Defendant has its principal place of business and headquarters in this District.

IV. FACTUAL BACKGROUND

A. The Data Breach

21. As outlined above, Patelco admitted that its vendor was the subject of a massive data breach that affected hundreds of thousands of its customers. On May 31, 2023, Defendant announced that "a previously unknown vulnerability in its MOVEit Transfer application (SecureFT)" was "exploited" and that through this exploit, "unauthorized actors" were able to use this "vulnerability to download a file containing" Plaintiff and Class Members' PII.[3]

22. The customer, and customer's family members', PII the hackers accessed include, but is not limited to, names and Social Security numbers.[4]

23. Patelco 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

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/9b39fcf4-1dfb-4b64-b5ef-c8144121f70f.shtml (last visited on October 2, 2023).
[3] *Id.*
[4] *Id.*

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

24. Patelco also promises to keep the PII it collects secure, even when it provides that PII to third parties. In its Privacy Policy, Patelco promises that "[t]he security of your personal and financial information is our highest priority."[5] Indeed, Patelco promises "[t]o protect [customers'] personal information from unauthorized access and use" by using "security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. Credit Union staff, management and volunteers are trained to keep consumer information strictly confidential."[6]

25. As a result of the Data Breach, Patelco is urging affected consumers to "remain vigilant against attempts at identity theft or fraud, which includes carefully reviewing online and financial accounts, credit reports, and Explanations of Benefits ("EOBs") from your health insurers for suspicious activity."[7] Furthermore, numerous data security experts are also suggesting that affected consumers take steps to protect their identities.

B. Plaintiff Expected Patelco and its Vendors to Keep Her Information Secure.

Plaintiff Sophie Jani's Experience

26. Plaintiff Sophie Jani, and her minor daughter, are customers of, and have accounts with, Patelco.

[5] *See* Patelco's Privacy Policy, *available at* https://www.patelco.org/privacy/ (last visited on October 2, 2023).
[6] *See* Patelco's Federal Privacy Notice, *available* at https://www.patelco.org/wp-content/uploads/2023/05/Federal-Privacy-Notice.pdf (last visited on October 2, 2023).
[7] *See Supra*, at Note No. 2.

27. Plaintiff Jani provided her PII, at Patelco's request, when she opened her account with Defendant in or around mid-2019. Plaintiff Jani provided her minor daughter's PII, at Patelco's request, when she opened an account for her minor daughter in late-2020.

28. Plaintiff Jani is very careful about sharing her, and her minor daughter's, sensitive Private Information. Plaintiff Jani has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

29. Plaintiff Jani, and her minor daughter, first learned of the Data Breach after each of them received Notice of Data Breach letters from Defendant on or around September 20, 2023, notifying them that Defendant suffered the Data Breach Defendant announced roughly four months prior and that their PII had been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

30. The Notice of Data Breach letters to Plaintiff Jani and her minor daughter indicated that the PII involved in the Data Breach included their names, addresses, emails, Social Security numbers, Patelco account numbers, dates of birth, phone numbers, and Driver's License numbers.

31. As a result of the Data Breach, Plaintiff Jani made reasonable efforts to mitigate the impact of the Data Breach after receiving the Notice of Data Breach letter, including but not limited to researching the Data Breach, reviewing credit reports, and financial account statements for any indications of actual or attempted identity theft or fraud.

32. Plaintiff Jani has spent multiple hours and will continue to spend valuable time for the remainder of her life, that she otherwise would have spent on other activities, including but not limited to work and/or recreation. Plaintiff Jani has already spent more than 4 hours trying to fix issues stemming from the Data Breach.

33. Plaintiff Jani, and her minor daughter, suffered actual injury from having their PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Defendant maintained belonging to Plaintiff Jani and her minor daughter; (b) violation of their privacy rights; (c) the theft of their

PII; and (d) present, imminent and impending injury arising from the increased risk of identity theft and fraud. In fact, because her, and her minor daughter's, Social Security numbers were impacted, Plaintiff Janina and her minor daughter, face this risk for their respective lifetimes.

34. As a result of the Data Breach, Plaintiff Jani has also suffered emotional distress as a result of the release of her and her minor daughter's PII, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her and her minor daughter's PII for purposes of identity theft and fraud. Plaintiff Jani is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

35. As a result of the Data Breach, Plaintiff Jani anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. In addition, Plaintiff Jani, and her minor daughter, will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of their respective lifetimes.

C. FTC Security Guidelines Concerning PII

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

37. 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.

38. 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.

39. 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.

40. 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.

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

42. 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]

43. Patelco 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

[8] *Privacy and Security Enforcement*, Fed. Trade Comm'n, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited on October 2, 2023).

steps to protect customers from unauthorized access. Among other violations, Patelco violated its obligations under Section 5 of the FTC Act.

D. Patelco Failed to Comply with the Gramm-Leach-Bliley Act

44. Patelco is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

45. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

46. Patelco collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Patelco was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

47. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

48. Accordingly, Patelco' conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

49. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy

policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Patelco violated the Privacy Rule and Regulation P.

50. Upon information and belief, Patelco failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on its network systems as well as those of its vendors.

51. Patelco failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

52. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring,

changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

53. As alleged herein, Patelco violated the Safeguards Rule.

54. Patelco failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its vendors or verify the integrity of those systems.

55. Patelco violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members: (a) an opt-out notice, and (b) a reasonable opportunity to opt out of such disclosure.

E. Patelco Was on Notice of Data Threats and the Inadequacy of Its Vendor's Data Security.

56. Patelco 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.

57. At all relevant times, Patelco 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, Patelco 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 Patelco should have anticipated and guarded against.

58. It is well known among financial institutions 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, UpGuard noted that "Cybercriminals choose their targets based on two conditions - maximum impact and maximum profit. Financial institutions perfectly meet these conditions because they store highly valuable data, and their

digital transformation efforts are creating greater opportunities for cyber attackers to access that data. This is why the financial sector is disproportionately targeted by cybercriminals"[9]

59. 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), Patelco knew or should have known that its electronic records would be targeted by cybercriminals.

60. 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.

F. The Data Breach Harmed Plaintiff and Class Members

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

62. 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.

63. 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.

[9] Edward Kost, *10 Biggest Data Breaches in Finance*, UPGUARD (Aug. 3, 2023), https://www.upguard.com/blog/biggest-data-breaches-financial-services (last visited on October 2, 2023).

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

65. 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.

66. Patelco has also vaguely stated that it "immediately took the affected application offline and activated [its] incident response procedures" without giving any details of what steps, exactly, it took.[10] Patelco also stated that they engaged with "[o]utside advisors and cybersecurity experts were retained to assist in the evaluation of the situation" again, without giving any details of who these advisors were, how they assisted, or any details about the Data Breach and the steps they took to ensure Plaintiff's and Class Members' PII cannot be accessed against.[11] Indeed, Plaintiff and Class Members are thus left to guess whether Patelco has, in fact, addressed the root causes of the Data Breach to ensure that Plaintiff and Class Members' PII cannot be accessed again.

67. Patelco'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.

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

[10] *See Supra*, at Note No. 2.
[11] *Id.*

69. 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 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.[12]

70. Criminals can use the PII that Patelco 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.[13]

71. 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.

72. 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."

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

74. 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

[12]https://www.cnet.com/tech/services-and-software/t-mobile-gets-hacked-again-is-the-uncarrier-un-safe/ (last visited on October 2, 2023).

[13] *See* https://consumer.ftc.gov/features/imposter-scams (last visited on October 2, 2023).

legal and regulatory frameworks."[14] American companies are estimated to have spent over $19 billion on 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.

75. 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.

76. 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.

77. 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 visited on October 2, 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 visited on October 2, 2023).

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

78. 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.

79. 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.

80. 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.

81. 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).

82. 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

[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 visited on October 2, 2023).

"once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[17]

83. Plaintiff and Class Members have failed to receive the value of the Patelco services for which they paid.

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

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

85. Patelco 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.

86. 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.

87. 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.

88. 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.

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

[17] *See* https://www.gao.gov/assets/gao-07-737.pdf (last visited on October 2, 2023).

90. 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.

91. 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, Patelco's vendor—for whom Patelco was responsible—left Plaintiff's and Class Members' PII vulnerable to access and theft, which is what ultimately happened.

92. The Data Breach was a reasonably foreseeable consequence of Defendant's failure to ensure that its vendors used adequate security systems. Patelco certainly has the resources to ensure that its vendors implement reasonable security systems to prevent or limit damage from data breaches. Even so, Patelco failed to properly invest in that data security. Had Patelco 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.

93. Patelco'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.

94. 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.

95. Even though Patelco 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.

96. 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.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

98. Specifically, Plaintiff proposes the following Nationwide Class, subject to amendment as appropriate:

> All individuals in the United States whose PII was impacted as a result of the Data Breach (the "Nationwide Class").

99. Plaintiff also proposes the following California Subclass, subject to amendment as appropriate:

> All individuals whose PII was impacted as a result of the Data Breach and resided in California at the time of the Data Breach (the "California Subclass").

100. The Nationwide Class and the California Subclass shall be collectively referred to herein as the "Class" unless otherwise specified.

101. Excluded from the Class are Patelco and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any judge to whom this case is assigned as well as their judicial staff and immediate family members.

102. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

103. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

104. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of Class Members is unknown to Plaintiff, upon information and belief approximately 181,507 individuals were impacted in the Data Beach. Thus, numerosity is met.

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

a. Whether Patelco engaged in the conduct alleged herein;

b. Whether Patelco's conduct violated the FTCA and/or GBLA;

c. When Patelco learned of the Data Breach;

d. Whether Patelco's response to the Data Breach was adequate;

e. Whether Patelco unlawfully lost or disclosed Plaintiff's and Class Members' PII;

f. Whether Patelco failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PII compromised in the Data Breach;

g. Whether Patelco's and its vendor's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Patelco's and its vendor's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Patelco owed a duty to Plaintiff and Class Members to safeguard their PII;

j. Whether Patelco breached its duty to Plaintiff and Class Members to safeguard their PII;

k. Whether hackers obtained Plaintiff's and Class Members' PII via the Data Breach;

l. Whether Patelco had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Patelco breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Patelco knew or should have known that its and its vendor's data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Patelco's misconduct;

p. Whether Patelco's conduct was negligent;

q. Whether Patelco was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

106. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data

Breach. Plaintiff's claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Patelco. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

107. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

108. Predominance. Patelco has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same vendor's computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Patelco's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

109. Superiority. A class action is superior to other available methods 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. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore 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, which would establish incompatible standards of conduct for Patelco. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

110. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Patelco has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

111. Finally, all members of the proposed Class are readily ascertainable. Patelco has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Patelco.

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

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

113. Patelco requires its customers, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its services.

114. Patelco gathered, stored, and shared the PII of Plaintiff and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

115. Plaintiff and Class Members entrusted Patelco with their PII, directly or indirectly, with the understanding that Patelco would safeguard their information.

116. Patelco had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

117. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Patelco had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Patelco's duty included a responsibility to exercise due diligence in selecting vendors and to audit, monitor, and ensure the integrity of its vendors' systems and practices and to give prompt notice to those affected in the case of a data breach.

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

119. Patelco's duty to use reasonable security measures also arose under the GLBA, under which it was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

120. Patelco owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its and its vendor's systems and networks, and the personnel responsible for them, adequately protected the PII.

121. Patelco's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Patelco and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Patelco with their confidential PII, a necessary part of being customers of Patelco.

122. Patelco's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Patelco is bound by industry standards to protect confidential PII.

123. Patelco was subject to an "independent duty," untethered to any contract between Patelco and Plaintiff or the Class.

124. Patelco also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII when it was no longer required to retain pursuant to regulations.

125. Moreover, Patelco had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

126. Patelco had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within its or its vendor's possession might have been compromised, how

it was compromised, and precisely the types of data that were compromised and when. Such notice was and is necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

127. Patelco breached its duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Patelco include, but are not limited to, the following:

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

b. Failing to adequately monitor the security of its and its vendor's networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

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

e. Failing to detect in a timely manner that Plaintiff's and Class Members' PII had been compromised;

f. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Plaintiff and Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

128. Patelco violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Patelco's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

129. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

130. Patelco's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

131. 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 Plaintiff and the Class.

132. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Patelco's inadequate security practices.

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

134. Patelco has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

135. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Patelco knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on its and its vendor's systems.

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

137. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Patelco's and its vendor's possession.

138. Patelco was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

139. Patelco's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

140. Patelco has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

141. But for Patelco's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

142. There is a close causal connection between Patelco's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Patelco's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

143. Patelco's conduct, as alleged herein, allowed it to gain a competitive advantage over companies offering the same or similar services because, rather than properly implement data security protocols, or verify the integrity of its vendor's systems, as required by statute and industry standards, Patelco diverted money intended to apply to data security towards its own profit. Patelco's conduct, and the unfair advantage realized thereby, creates a race to the bottom by encouraging companies to divert funds intended for data security towards profits in order to remain competitive. The end effect is that both consumers and the marketplace in general are harmed through the widespread adoption of substandard data security practices and the concomitantly increased risk of cyberattacks and fraud and identity theft (which disrupt the lives of victims and impose a burden on the state to investigate and prevent criminal activity).

144. By collecting and taking custody of Plaintiff's and Class Members' PII with full awareness of both the likelihood of a cyberattack targeted to acquire that information and the

severe consequences that would result to Plaintiff and Class Members if the confidentiality of the PII was breached, Patelco assumed a special relationship that required it to guard against the foreseeable conduct of a criminal third party. If Patelco had not intervened by taking charge of Plaintiff's and Class Member's PII, no harm would have resulted to Plaintiff and Class Members as a result of the Data Breach.

145. As a direct and proximate result of Patelco's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Patelco's and its vendor's possession and is subject to further unauthorized disclosures so long as Patelco fails to undertake appropriate and adequate measures to protect the PII.

146. As a direct and proximate result of Patelco's negligence, Plaintiff and the Class 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.

147. Additionally, as a direct and proximate result of Patelco's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Patelco's and its vendor's possession and is subject to further unauthorized disclosures so long as Patelco fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

148. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

149. Patelco's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

150. Plaintiff and Class Members are also entitled to injunctive relief requiring Patelco to: (i) strengthen its and its vendor's data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

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

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

152. 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.

153. 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.

154. 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.

155. 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.

156. 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
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

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

158. Plaintiff and Class Members conferred a monetary benefit on Patelco.

159. Specifically, they paid for services from Patelco and/or its agents and in so doing also provided Patelco with their PII. In exchange, Plaintiff and Class Members should have received from Patelco the services that were the subject of the transaction and should have had their PII protected with adequate data security.

160. Patelco knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Patelco profited from Plaintiff's and Class Members' retained data and used Plaintiff's and Class Members' PII for business purposes.

161. Patelco failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

162. Patelco acquired the PII through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

163. If Plaintiff and Class Members had known that Patelco would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Patelco or obtained services at Patelco.

164. Plaintiff and Class Members have no adequate remedy at law.

165. Under the circumstances, it would be unjust for Patelco to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

166. As a direct and proximate result of Patelco's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; (v) and

increase in spam calls, texts, and/or emails; and (vi) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Patelco's possession and is subject to further unauthorized disclosures so long as Patelco fails to undertake appropriate and adequate measures to protect the PII.

167. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Patelco and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Patelco from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

168. Plaintiff and Class Members may not have an adequate remedy at law against Patelco, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, *et. seq.* ("CCPA")
(On Behalf of Plaintiff and the California Subclass)

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

170. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devasting effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."

171. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

172. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party 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." Cal. Civ. Code § 1798.81.5(c).

173. Section 1798.150(a)(1) of the CCPA provides:

> "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper."

174. Plaintiff and California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

175. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

176. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff's and California Subclass Members' unencrypted first and last names and Social Security numbers among other information.

177. Plaintiff and California Subclass Members' PII was subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and contact information was wrongfully taken, accessed, and viewed by an unauthorized third party.

178. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff's and California Subclass Members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff's and California Subclass Members' PII as a result of this attack.

179. On October 2, 2023, Plaintiff provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant fails to respond, or has not cured, or is unable to cure the violation within 30 days thereof, Plaintiff will amend this Complaint to seek all relief available under the CCPA including damages to be measured as

the greater of actual damages or statutory damages in an amount up to seven hundred and fifty dollars ($750) per consumer per incident. See Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

180. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT V
California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*
(On Behalf of Plaintiff and the Class)

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

182. Defendant's acts and omissions as alleged herein emanated and directed from California.

183. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

184. Defendant stored the PII of Plaintiff and Class Members in its computer systems.

185. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with federal regulations and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of that PII.

186. Defendant did not disclose at any time that Plaintiff's and Class Members' PII was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only one in possession of that material information, which Defendant had a duty to disclose.

Unlawful Business Practices

187. As noted above, Defendant violated Section 5(a) of the FTC Act (which is a predicate legal violation for this UCL claim) by misrepresenting, by omission, the safety of its

computer systems, specifically the security thereof, and its ability to safely store Plaintiff's and Class Members' PII.

188. Defendant also violated Section 5(a) of the FTC Act by failing to implement reasonable and appropriate security measures or follow industry standards for data security.

189. If Defendant had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach, and consequently from Defendant's failure to timely notify Plaintiff and Class Members of the Data Breach.

190. Defendant's acts and omissions as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the FTC Act.

191. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In addition, Plaintiff's and Class Members' PII was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

Unfair Business Practices

192. Defendant engaged in unfair business practices under the "balancing test." The harm caused by Defendant's actions and omissions, as described in detail above, greatly outweighs any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and failure to disclose inadequacies of Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged below.

193. Defendant engaged in unfair business practices under the "tethering test." Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to

them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

194. Defendant engaged in unfair business practices under the "FTC test." The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects hundreds of thousands of Class Members and has caused those persons to suffer actual harm. Such harms include a substantial risk of identity theft, disclosure of Plaintiff's and Class Members' PII to third parties without their consent, diminution in value of their PII, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiff's and Class Members' PII remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated Section 5(a) of the Federal Trade Commission Act. See 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"); *see also, e.g., In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated §5(a) of FTC Act).

195. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. Plaintiff's and Class Members' PII was taken and in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services,

identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

196. As a result of Defendant's unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to damages, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their counsel to represent the Class;

B. For equitable relief enjoining Patelco from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Patelco to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Patelco from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Patelco to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Patelco to delete, destroy, and purge the PII of Plaintiff and Class Members unless Patelco can provide to the Court reasonable justification for

the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Patelco to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. Prohibiting Patelco from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Patelco to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on its and its vendor's systems on a periodic basis, and ordering Patelco to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Patelco to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Patelco to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Patelco to segment data by, among other things, creating firewalls and access controls so that if one area of its network is compromised, hackers cannot gain access to other portions of its systems;

x. Requiring Patelco to conduct regular database scanning and securing checks;

xi. Requiring Patelco to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. Requiring Patelco to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to

identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Patelco to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with its policies, programs, and systems for protecting PII;

xiv. Requiring Patelco to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor its information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Patelco to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Patelco to implement logging and monitoring programs sufficient to track traffic to and from its servers; and

xvii. For a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Patelco's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Patelco's wrongful conduct;

F. Ordering Patelco to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

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

Dated: October 2, 2023

Respectfully Submitted,

By: */s/ M. Anderson Berry*

M. Anderson Berry
Gregory Haroutunian
Brandon P. Jack
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com
bjack@justice4you.com

Attorneys for Plaintiff and the Proposed Class