RACHELE R. BYRD (190634)
byrd@whafh.com
ALEX J. TRAMONTANO (276666)
tramontano@whafh.com
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599

Attorneys for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOSH WARREN, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

PATELCO CREDIT UNION,

Defendant.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Josh Warren, by and through his counsel, brings this Class Action Complaint against Defendant Patelco Credit Union ("Defendant" or "Patelco"), individually and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his 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, and upon information and belief, their names, dates of birth, addresses, Social Security numbers, driver's license numbers, and/or financial account information (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.

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 names, dates of birth, addresses, Social Security numbers, driver's license numbers, and/or financial account information.

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 consumers' PII safe and confidential.

[1] *See* https://www.patelco.org/about-patelco/who-we-are/ (last visited July 2, 2024).

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.

9. On or about June 30, 2024, Patelco began sending Plaintiff and other Class Members an email communication (the "Notice Email") informing them that on June 29, 2024 Patelco suffered a serious security incident that required it to shut down its day-to-day banking systems to remediate the issue and contain the impact (the "Data Breach").[2] As a result of this Data Breach, Patelco's online banking, mobile app, and call center were shut down; electronic transactions were, and currently still are, unavailable; and debit and credit card transactions are being limited by Patelco.[3] As a result of the Data Breach, Plaintiff and Class Members have lost access to their money and financial accounts.

10. Moreover, because of the Data Breach and resulting service outages stemming therefrom, Defendant has been encouraging Plaintiff and Class Members to travel to and from various Patelco ATM locations to withdraw or deposit their money thereby causing Plaintiff and Class Members to incur out-of-pocket travel expenses (including but not limited to gasoline/fuel expenses and wear and tear on their personal vehicles). Specifically, Defendant urges Plaintiff and Class Members to travel to their local ATMs stating, "For cash withdrawals and deposits, you can access Patelco ATMS, including over 30,000 shared branch ATMS in the U.S. Find your nearest branch and ATM (including hours of operation) at patelco.org/locations."[4]

11. On or about July 1, 2024, Patelco provided another email update and an update on its website stating that the "serious security incident" was in fact a ransomware attack.[5]

---

[2] *See* Aidin Vaziri, *Bay Area credit union Patelco hit by 'serious security incident,' banking disrupted*, *available at* https://www.sfchronicle.com/bayarea/article/patelco-credit-union-security-breach-outage-19549333.php (last visited July 2, 2024); *see also* https://www.patelco.org/securityupdate (last visited July 2, 2024).

[3] *Id.*

[4] *Id.*

[5] *Id.*

Patelco has still not provided any information to Plaintiff and Class Members regarding any details as to which types of PII were stolen in the Data Breach.

12. Ransomware attacks, by their very nature, almost never occur without the cybercriminal perpetrator(s) accessing, and indeed, exfiltrating, PII from the target.

13. Upon information and belief, Plaintiff's and Class Members' PII has been exposed and exfiltrated as a result of this Data Breach.

14. Noticeably absent from the Notice Email 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.

15. Upon information and belief, the attacker accessed and acquired files that Patelco stored on its systems containing unencrypted PII of Plaintiff and Class Members, including but not limited to their Social Security numbers.

16. 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 state and federal statutes.

17. 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 travel expenses and 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; (v) loss of access to their money and financial accounts; and (vi) 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.

18. 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

19. Plaintiff Josh Warren is, and at all times relevant, has been a citizen of Livermore, California. Plaintiff Warren has no intention of moving to a different state in the immediate future. Plaintiff Warren received emails from Defendant notifying him of the Data Breach on or around June 30, 2024 and July 1, 2024 respectively.

20. On or about July 3, 2024, pursuant to § 1798.150(b) of the CCPA, Plaintiff Warren separately provided written notice to Defendant identifying the specific provisions of this title he 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).

21. 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

22. 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. Thus, minimal diversity exists under 28 U.S.C. §1332(d)(2)(A).

23. 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.

24. 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

25. As outlined above, Patelco admitted that on June 29, 2024, it suffered a serious security incident. Specifically, on June 30, 2024, Defendant emailed Plaintiff and Class Members and announced that it was the victim of a Data Breach stating that "[w]e are writing to let you know that on June 29, we experienced a serious security incident. This required us to shut down some of our day-to-day banking systems so that we can remediate the issue and contain the impact, including online banking, our mobile App, and our call center. Currently, electronic transactions such as transfers (including Zelle), direct deposit, balance inquiries, and payments are unavailable."[6]

[6] *See supra,* fn. 2.

26. Moreover, Defendant further clarified in a security update and in emails to Plaintiff and Class Members on July 1, 2024, that the Data Breach was in fact a ransomware attack.[7]

27. Upon information and belief, customer PII the hackers accessed and exfiltrated in the Data Breach includes, but is not limited to, Plaintiff's and Class Members' names, dates of birth, addresses, Social Security numbers, driver's license numbers, and/or financial account information.

28. 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 vendors would protect that PII. 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.

29. Indeed, Patelco understands the importance of keeping its customer's PII safe and is uniquely aware of the prevalence of Data Breaches suffered by financial institutions because Patelco suffered a large data breach approximately one year ago and a lawsuit was filed against Patelco for that data breach.[8]

30. 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."[9] 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

---

[7] *Id.*

[8] *See Jani v. Patelco Credit Union*, No. 3:23-cv-05054-RFL (N.D. Cal.), filed October 2, 2023.

[9] *See* Patelco's Privacy Policy, *available at* https://www.patelco.org/privacy/ (last visited July 2, 2024).

secured files and buildings. Credit Union staff, management and volunteers are trained to keep consumer information strictly confidential."[10]

31. Due to Defendant's inadequate and insufficient data security measures, Plaintiff and Class Members now face an increased risk of fraud and identity theft and must live with that threat forever. Since the Data Breach happened, Plaintiff has experienced a significant increase of spam emails and has suffered an unknown individual attempting to register his credit card on an e-commerce site and it charged him with a registration/verification fee of approximately $10. Plaintiff has also suffered being locked out of his Patelco financial accounts as a result of the Data Breach. Plaintiff believes his PII was both stolen in the Data Breach and is still in the hands of cybercriminals. Plaintiff further believes his PII has already been sold on the Dark Web and downloaded following the Data Breach, as that is the *modus operandi* of cybercriminals who perpetrate cyberattacks of the type that occurred here.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties, and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

33. Defendant had obligations created by contract, industry standards, federal law, common law, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

34. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

35. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access and disclosure.

[10] *See* Patelco's Federal Privacy Notice, *available* at https://www.patelco.org/wp-content/uploads/2023/05/Federal-Privacy-Notice.pdf (last visited July 2, 2024).

36. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches of major companies preceding the date of the Data Breach.

37. Defendant knew or should have known that these attacks were common and foreseeable. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record, wherein 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records, a 68% increase from 2020.[11] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

38. Moreover, Defendant is uniquely aware of the prevalence of data breaches because it suffered a similar data security incident approximately one year ago.[13]

39. "The financial industry is a large target for many different groups – from organized criminals seeking to steal money to politically motivated groups attempting to make a statement."[14] Security experts have warned that "[a]lthough big banks are believed to have strong defenses, … hackers could infiltrate the industry through third parties with lax security."[15]

40. The increase in such attacks, and the resulting risk of future attacks, was widely known to the public and to anyone in the Defendant's industry, including Defendant.

FTC Security Guidelines Concerning PII

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

---

[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (*available at*: https://www.idtheftcenter.org/wp-content/uploads/2022/04/ITRC_2021_Data_Breach_Report.pdf), at 6 (last visited July 2, 2024).

[12] *See Id.; see also Data Breaches Hit Lots More People in 2022* (Jan. 25, 2023) *available at*: https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last visited July 2, 2024).

[13] *See supra*, fn. 3.

[14] Egan, Matt, *Hackers paralyzed a pipeline. Banks and stock exchanges are even bigger targets*, available at: https://www.cnn.com/2021/05/12/business/ransomware-attacks-banks-stock-exchanges/index.html (last visited Jul. 2, 2024).

[15] *Id.*

42. 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.

43. 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.

44. 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.

45. 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.

46. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website, 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.[16]

47. Defendant 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, Defendant violated its obligations under Section 5 of the FTC Act.

Defendant Failed to Comply with the Gramm-Leach-Bliley Act

48. Defendant 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.

49. 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).

50. Defendant 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.

51. 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

[16] *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 July 2, 2024).

Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

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

53. 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, Defendant violated the Privacy Rule and Regulation P.

54. 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.

55. Defendant 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.

56. 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.

57. As alleged herein, Defendant violated the Safeguards Rule.

58. Upon information and belief, Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor its systems or verify the integrity of those systems.

59. Defendant 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.

Defendant Did Not Use Reasonable Security Procedures

60. Despite this knowledge, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, non-encrypted, and non-redacted information it was maintaining for Plaintiff and Class Members, causing Plaintiff and Class Members' PII to be exposed and exfiltrated by cyber criminals.

61. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets,

employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling the Remote Desktop Protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

62. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters and keep them updated to reduce malicious network traffic.[17]

63. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> Secure internet-facing assets
>
> - Apply the latest security updates
> - Use threat and vulnerability management
>
> - Perform regular audit
> - Remove privileged credentials
>
> Thoroughly investigate and remediate alerts
>
> - Prioritize and treat commodity malware infections as potential full compromise.
>
> Include IT Pros in security discussions
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely.
>
> Build credential hygiene
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords.

[17] *See* Cybersecurity & Infrastructure Security Agency, *Protecting Against Ransomware* (original release date Apr. 11, 2019), *available at:* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited July 2, 2024).

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[18]

64. Given that Defendant was storing the PII of Plaintiff and Class Members, Defendant could and should have implemented all the above measures to prevent and detect cyber-attacks.

65. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent "hacking" attacks, resulting in the Data Breach and the exposure of the PII of an undisclosed amount of current and former consumers, including Plaintiff and Class Members.

Securing PII and Preventing Breaches

66. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

A. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

B. Failing to adequately protect customers' PII;

[18] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited July 2, 2024).

C. Failing to properly monitor its own data security systems for existing intrusions;

D. Failing to ensure that it, and its vendors with access to its computer systems and data, employed reasonable security procedures; and;

E. Failing to adhere to industry standards for cybersecurity.

67. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data that was no longer useful, especially outdated data.

68. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members was exacerbated by the repeated warnings and alerts directed to businesses to protect and secure sensitive data.

69. Despite the prevalence of public announcements of data breaches and data security compromises, including Defendant's own recent data breach, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

Defendant Failed to Comply with Industry Standards

70. Several best practices have been identified that, at a minimum, should be implemented by companies like Defendant, including but not limited to, educating all employees; 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. Defendant failed to follow these industry best practices.

71. 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 protecting physical security systems; protecting against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

Value of Personally Identifiable Information

72. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[22]

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

---

[19] *See Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited July 2, 2024).

[20] *See Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 2, 2024).

[21] *See In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 2, 2024).

[22] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 2, 2024).

75. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[23]

76. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—upon information and belief, name, date of birth, address, Social Security number, driver's license number, and/or financial account information.

77. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market."[24]

78. Among other forms of fraud, identity thieves may use Social Security numbers to obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

79. Moreover, the fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once

[23] *See* Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited July 2, 2024).

[24] *See* Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited July 2, 2024).

> stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

80. The PII stolen in the Data Breach has significant value, as PII is a valuable property right.[26] Sensitive PII can sell for as much as $363 per record, according to the Infosec Institute.[27]

81. There is also an active, robust, and legitimate marketplace for PII. In 2019, the data brokering industry was worth roughly $200 billion.[28] In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.[29] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60.00 a year.[30]

82. As a result of the Data Breach, Plaintiff's, and Class Members' PII, which has an inherent market value in both legitimate and black markets, has been damaged and diminished by its unauthorized release to third-party actors, to whom it holds significant value. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of Plaintiff's and Class Members' PII has been lost, thereby causing additional loss of value.

---

[25] *See Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited July 2, 2024).

[26] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets." (citations omitted)).

[27] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 2, 2024).

[28] *See* David Lazarus, *Shadowy Data Brokers Make the Most of Their Invisibility Cloak* (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 2, 2024).

[29] *See, e.g.*, https://datacoup.com/; *see also* https://worlddataexchange.com/about (last visited July 2, 2024.)

[30] *See* Computer & Mobile Panel, NIELSEN, *available at* https://computermobilepanel.nielsen.com/ui/US/en/sdp/landing (last visited July 2, 2024).

83. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including but not limited to name, date of birth, address, Social Security number, driver's license number, and/or financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach and the costs associated with being denied access to their money and financial accounts.

84. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Since the Data Breach, Plaintiff has been experiencing a significant uptick in spam emails and even fraud. Beyond the relentless stress and anxiety this situation has caused, Plaintiff has already devoted, and anticipated continuing to devote, countless hours to the vigilant monitoring of their identity and financial accounts to mitigate any potential harm. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

85. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s) and computer network, amounting to potentially tens of thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

86. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members, including, but not limited to, failing to encrypt sensitive PII, failing to redact sensitive PII, keeping unencrypted and unredacted sensitive PII in internet facing environments, and failing to delete sensitive PII Defendant had no reasonable business purpose for continuing to maintain. The ramifications of Defendant's failure to safeguard the PII of Plaintiff and Class Members are long-lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

V. PLAINTIFF-SPECIFIC ALLEGATIONS

Plaintiff Josh Warren's Experience

87. Plaintiff Warren is a customer of, and has an account with, Patelco.

88. Plaintiff Warren provided his PII, at Patelco's request, when he opened his account with Defendant.

89. Plaintiff Warren is very careful about sharing his sensitive Private Information. Plaintiff Warren has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

90. Plaintiff Warren first learned of the Data Breach after he received an email from Defendant on or around June 30, 2024, notifying him that Defendant suffered the Data Breach that reportedly occurred on June 29, 2024. Upon information and belief, Plaintiff Warren believes that his PII has been improperly accessed and/or obtained by unauthorized third parties while in possession of Defendant.

91. Upon information and belief, the PII involved in the Data Breach included at least Plaintiff Warren's name, date of birth, address, Social Security number, driver's license number, and/or financial account information.

92. As a result of the Data Breach, Plaintiff Warren made reasonable efforts to mitigate the impact of the Data Breach after receiving the Data Breach email, 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.

93. Plaintiff Warren has spent multiple hours and will continue to spend valuable time for the remainder of his life, that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

94. Plaintiff Warren has also suffered fraud as a result of the Data Breach. Specifically, an unknown individual attempted to register his credit card on an e-commerce site and it charged him with a registration/verification fee of approximately $10.

95. Plaintiff Warren suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant maintained belonging to Plaintiff Warren; (b) violation of his privacy rights; (c) the theft of his PII; (d) loss of access to his money and financial accounts; (e) actual tangible financial losses from the fraud he suffered as a result of the Data Breach; and (f) present, imminent and impending injury arising from the increased risk of identity theft and fraud. In fact, because his Social Security number was impacted, Plaintiff Warren faces this risk for the rest of his lifetime.

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

97. As a result of the Data Breach, Plaintiff Warren 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 Warren will continue to be at present, imminent, and continued increased risk of identity theft and fraud for the remainder of his lifetime.

Plaintiff's Injuries and Damages

98. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members are presently experiencing and will continue experiencing actual harm from fraud and identity theft.

99. Plaintiff and Class Members are presently experiencing substantial risk of out-of-pocket fraud losses, such as loans opened in their names, tax return fraud, utility and medical bills opened in their names, and similar identity theft.

100. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiff and Class Members.

101. Plaintiff and Class Members are also incurring and may continue incurring out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

102. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by the cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

103. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service than they otherwise would have, in exchange for which Defendant was supposed to provide adequate data security but was not. Part of the price Plaintiff and Class Members paid to Defendant and its affiliates was intended to be used by Defendant to fund adequate security of Defendant's computer property and protect Plaintiff's and Class Members' PII. Thus, Plaintiff and Class Members did not get what they paid for.

104. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

105. Plaintiff and Class Members have suffered actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of unauthorized credit card transactions, lost use of financial instruments, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent loans, insurance claims, tax returns, and/or government benefit claims;

b. Purchasing credit monitoring and identity theft prevention;

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

d. Spending time on the phone with or at a financial institution or government

agency to dispute fraudulent charges and/or claims;

e. Contacting financial institutions and closing or modifying financial accounts; and/or

f. Closely reviewing and monitoring medical insurance accounts, bank accounts, payment card statements, and credit reports for unauthorized activity for years to come.

106. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing sensitive and confidential personal, and/or financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

107. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

108. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and are at a substantial and present risk of harm.

VI. CLASS ACTION ALLEGATIONS

109. 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).

110. 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").

111. 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 were citizens of California at the time of the Data Breach (the "California Subclass").**

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

113. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

114. 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.

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

116. 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, at least tens of thousands, if not hundreds of thousands, of individuals were impacted in the Data Beach. Thus, numerosity is met.

117. 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 Defendant engaged in the conduct alleged herein;

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

c. When Defendant learned of the Data Breach;

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

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

f. Whether Defendant 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 Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

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

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

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

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

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

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

p. Whether Defendant conduct was negligent;

q. Whether Defendant 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.

118. 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 Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself 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.

119. 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.

120. Predominance. Defendant 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 its computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant'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.

121. 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 Defendant. 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.

122. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant 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. Finally, all members of the proposed Class are readily ascertainable. Defendant 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.

VII. CAUSES OF ACTION

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

123. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

124. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

125. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' PII.

126. Defendant 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.

127. Defendant'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.

128. Defendant 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 data were wrongfully disclosed.

129. By assuming responsibility for collecting and storing this data, and in fact doing so and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty includes, but is not limited to, a responsibility to redact and encrypt sensitive information, promptly remove sensitive information that's no longer needed, implement processes by which it could detect a breach of its security systems in a reasonably expeditious time period, and to give prompt notice to those affected in the case of a data breach.

130. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or Class Members.

131. A breach of security, unauthorized access, and resulting injury to Plaintiff's and Class Members' PII was reasonably foreseeable, particularly considering Defendant's inadequate security practices, which include sharing and/or storing the PII of Plaintiff and Class Members on its computer systems.

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

133. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the

steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with state and federal law and industry standards for the safekeeping of the PII of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

134. Plaintiff and Class Members had no ability to protect their PII that was in, and probably remains in, Defendant's possession.

135. Defendant was able to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

136. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

137. Defendant had a duty to comply with the laws and industry standards set out above.

138. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII within Defendant's possession.

139. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' PII.

140. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the PII within Defendant's possession might have been compromised and precisely the type of information compromised.

141. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' PII to be compromised.

142. Defendant 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 networks and systems;

c. Failing to audit, monitor, or ensure the integrity of its 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.

143. Defendant 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. Defendant'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.

144. 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.

145. Defendant's violation of Section 5 of the FTC Act and GLBA constitutes negligence.

146. 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.

147. As a result of Defendant's ongoing failure to notify Plaintiff and Class Members regarding the type of PII that has been compromised, Plaintiff and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

148. Defendant's breaches of duty caused Plaintiff and Class Members to suffer from identity theft, fraud, loss of time and money to monitor their finances for fraud, loss of access to their money and financial accounts, and loss of control over their PII.

149. As a result of Defendant's negligence and breach of duties, Plaintiff and Class Members are in danger of present and continuing harm in that their PII, which is still in the possession of third parties, will be used for fraudulent purposes. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the PII at issue, which upon information and belief includes Social Security numbers.

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

151. Plaintiff seeks the award of actual damages on behalf of himself and the Class.

152. In failing to secure Plaintiff's and Class Members' PII and promptly notifying them of the Data Breach, Defendant is guilty of oppression, fraud, or malice, in that Defendant acted or failed to act with a willful and conscious disregard of Plaintiff's and Class Members' rights. Plaintiff, therefore, in addition to seeking actual damages, seeks punitive damages on behalf of himself and the Class.

153. Plaintiff seeks injunctive relief on behalf of the Class in the form of an order compelling Defendant to institute appropriate data collection and safeguarding methods and policies regarding customer information.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

154. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

155. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by companies like Defendant of failing to use reasonable measures to protect PII.

156. The FTC publications and orders also form the basis of Defendant's duty to the Class.

157. Additionally, the California Consumer Privacy Act ("CCPA"), specifically, Civil Code §§ 1798.81.5 and 1798.150, require that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

158. Defendant violated Section 5 of the FTC Act and the CCPA (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach of that data.

159. Defendant's violation of Section 5 of the FTC Act and CCPA (and similar state statutes) constitutes negligence *per se*.

160. Class Members are consumers within the class of persons Section 5 of the FTC Act and CCPA (and similar state statutes) was intended to protect.

161. Moreover, the harm that has occurred is the type of harm the FTC Act and CCPA (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty

enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

162. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

163. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

164. Plaintiff and Class Members conferred a monetary benefit to Defendant by paying Defendant, and entrusting money to Defendant, for various services relating to its business.

165. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant by entering into a business relationship. Defendant acknowledged and retained this benefit when it accepted the terms of this relationship with Plaintiff and Class Members.

166. Defendant was supposed to use some of the monetary benefit provided to it from Plaintiff and Class Members to secure the PII belonging to Plaintiff and Class Members by paying for costs of adequate data management and security.

167. Defendant should not be permitted to retain any monetary benefit as a result of its failure to implement necessary security measures to protect the PII of Plaintiff and Class Members.

168. Defendant gained access to Plaintiff's and Class Members' PII through inequitable means because Defendant failed to disclose that it used inadequate security measures.

169. Plaintiff and Class Members were unaware of the inadequate security measures and would not have provided their PII to Defendant had they known of the inadequate security measures.

170. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

171. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise and/or theft of their PII; (iv) out-of-pocket expenses associated with travel expenses and the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain 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 of Plaintiff and Class Members; (viii) loss of access to their money and financial accounts; and (ix) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

173. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds from the monetary benefit that it unjustly received from them.

FOURTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

174. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

175. Plaintiff and the Class, encompassing clients, business relations, and claimants of Defendant, delivered their PII to Defendant as part of the process of engaging in financial and other transactions.

176. Upon providing their PII in exchange for professional opportunities, financial services, or other transactions, Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Member's data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

177. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

178. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

179. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

180. Defendant accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing financial services or other business services to Plaintiff and Class Members.

181. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

182. Defendant recognized that the PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

183. Plaintiff and the Class fully performed their obligations under the implied contract with Defendant.

184. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard their data.

185. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and acquisition of their PII.

186. As a direct and proximate result of the breach of the contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's and Class Members' PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed classes entrusted Defendant with their PII; (h) loss of access to their money and financial accounts; and (i) the continued and substantial risk to Plaintiff's and Class Members' PII, which remains in the Defendant's possession of Defendant with in-adequate measures to protect Plaintiff's and Class Members' PII.

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

187. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

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

189. 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*.

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

191. 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.

192. 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

193. 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.

194. 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.

195. 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.

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

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

Unfair Business Practices

198. 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.

199. 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.

200. 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, travel expenses, 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).

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

202. 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.

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

203. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

204. 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."

205. 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.

206. 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).

207. 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.

208. 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."

209. 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.

210. 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.

211. 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.

212. 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 its server or network by hackers and to prevent unauthorized access of Plaintiff's and California Subclass Members' PII as a result of this attack.

213. On or about July 3, 2024, 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).

214. 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.

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. 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, Class Members, and the public at large including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. requiring Defendant to delete, destroy, and purge the PII of Plaintiff, Class Members, and all members of the public whose PII Defendant retains or may retain in the future unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff, Class Members, and the public at large;

iv. requiring Defendant to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff, Class Members, and any member of the public at large whose PII Defendant possesses, or may come to possess, in the future;

vi. prohibiting Defendant from maintaining the PII of Plaintiff, Class Members, and any member of the public at large whose PII Defendant possesses, or may come to possess, in the future on a cloud-based database;

vii. requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and securing checks;

xii. requiring Defendant 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff, Class Members, and any member of the public at large whose PII Defendant possesses, or may come to possess, in the future;

xiii. requiring Defendant 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;

xiv. requiring Defendant 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 Defendant's policies, programs, and systems for protecting

personal identifying information;

xv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xvi. requiring Defendant 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;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and 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 Defendant'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;

D. For an award of damages, including actual, nominal, statutory, treble, consequential, and punitive damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Dated: July 3, 2024 Respectfully Submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP

By: */s/ Rachele R. Byrd*
RACHELE R. BYRD (190634)
byrd@whafh.com
ALEX J. TRAMONTANO (276666)
tramontano@whafh.com
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: 619/239-4599
Facsimile: 619/234-4599

Attorneys for Plaintiff and the Proposed Class