

1 Daniel Srourian, Esq. [SBN 285678]  
2 **SROURIAN LAW FIRM, P.C.**  
3 468 N. Camden Dr., Suite 200  
4 Beverly Hills, CA 90210  
Telephone: (213) 474-3800  
Fax: (213) 471-4160  
Email: daniel@slfla.com

Attorneys for Representative Plaintiff

6 **UNITED STATES DISTRICT COURT**  
7 **NORTHERN DISTRICT OF CALIFORNIA**

8 TAMRA BACON, individually,  
9 and on behalf of all others  
10 similarly situated,

Plaintiffs,

11 vs.

12 WELLS FARGO BANK, N.A.,  
13 Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT**  
**JURY TRIAL DEMANDED**

14  
15 Representative Plaintiff alleges as follows:

16 **INTRODUCTION**

17 1. Representative Plaintiff Tamra Bacon (“Representative Plaintiff”)  
18 brings this Class Action Complaint against Defendant Wells Fargo Bank, N.A.  
19 (“Defendant” or “WF”) for its failure to properly secure and safeguard  
20 Representative Plaintiff’s and Class Members’ personally identifiable information  
21 stored within Defendant’s information network, including, without limitation, full  
22 names, address, phone number, email address, dates of birth, driver’s license  
23 number, bank account number(s), credit/debit card number, brokerage account  
24

1 number(s), and/or loan/line of credit number(s) and Social Security numbers  
2 (these types of information, *inter alia*, being thereafter referred to, collectively, as  
3 “personally identifiable information” or “PII”).<sup>1</sup>

4           2. With this action, Representative Plaintiff seeks to hold Defendant  
5 responsible for the harms it caused and will continue to cause Representative  
6 Plaintiff and, at least, thousands of other similarly situated persons in the  
7 preventable hack purportedly discovered by Defendant on or around July 2024, in  
8 which unauthorized actors accessed Defendant’s inadequately protected network  
9 servers and accessed highly sensitive PII that was being kept unprotected (“Data  
10 Breach”).  
11

12           3. Defendant acquired, collected, and stored Representative Plaintiff’s  
13 and Class Members’ PII. Therefore, at all relevant times, Defendant knew or  
14 should have known that Representative Plaintiff and Class Members would use  
15 Defendant’s services to store and/or share sensitive data, including highly  
16 confidential PII.  
17

18           4. By obtaining, collecting, using, and deriving a benefit from  
19 Representative Plaintiff’s and Class Members’ PII, Defendant assumed legal and  
20

21  
22  
23 <sup>1</sup> Personally identifiable information (“PII”) generally incorporates information that can be used to  
24 distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying  
information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an  
individual. PII also is generally defined to include certain identifiers that do not on its face name an individual,  
but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social  
Security numbers, passport numbers, driver’s license numbers, financial account numbers, etc.).

1 equitable duties to those individuals. These duties arise from state and federal  
 2 statutes and regulations, and common law principles.

3           5. Defendant disregarded the rights of Representative Plaintiff and  
 4 Class Members by intentionally, willfully, recklessly, and/or negligently failing to  
 5 take and implement adequate and reasonable measures to ensure that  
 6 Representative Plaintiff’s and Class Members’ PII was safeguarded, failing to  
 7 take available steps to prevent unauthorized disclosure of data and failing to  
 8 follow applicable, required and appropriate protocols, policies, and procedures  
 9 regarding the encryption of data, even for internal use. As a result, Representative  
 10 Plaintiff’s and Class Members’ PII was compromised and, as admitted to by  
 11 Defendants, in some cases used for fraudulent purposes. Representative Plaintiff  
 12 and Class Members have a continuing interest in ensuring that their information is  
 13 and remains safe and are entitled to injunctive and other equitable relief.

14  
 15  
 16                               **JURISDICTION AND VENUE**

17           6. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity  
 18 jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction  
 19 over this action under 28 U.S.C. § 1332(d) because this is a class action where the  
 20 amount in controversy exceeds the sum or value of \$5 million, exclusive of  
 21 interest and costs, there are more than 100 members in the proposed class, and at  
 22 least one Class Member is a citizen of a state different from Defendant.  
 23  
 24

1           7.       Supplemental jurisdiction to adjudicate issues pertaining to state law  
2 is proper in this Court under 28 U.S.C. § 1367.

3           8.       Defendant is headquartered and/or routinely conducts business in the  
4 State where this District is located, has sufficient minimum contacts in this State,  
5 has intentionally availed itself of this jurisdiction by marketing and/or selling  
6 products and/or services and/or by accepting and processing payments for those  
7 products and/or services within this State.

9           9.       Venue is proper in this Court under 28 U.S.C. § 1391 because a  
10 substantial part of the events that gave rise to Representative Plaintiff's claims  
11 took place within this District and Defendant is headquartered and/or does  
12 business in this Judicial District.

13  
14           **REPRESENTATIVE PLAINTIFF'S COMMON EXPERIENCES**

15           10.       Defendant received highly sensitive PII from Representative Plaintiff  
16 in connection with the services Representative Plaintiff received or requested. As  
17 a result, Representative Plaintiff's information was among the data an  
18 unauthorized third party accessed in the Data Breach.

19  
20           11.       Representative Plaintiff was and is very careful about sharing her  
21 PII. Representative Plaintiff have never knowingly transmitted unencrypted  
22 sensitive PII over the internet or any other unsecured source.

23           12.       Representative Plaintiff stored any documents containing their PII in  
24 a safe and secure location or destroyed the documents. Moreover, Representative

1 Plaintiff diligently chose unique usernames and passwords for their various online  
2 accounts.

3 13. Representative Plaintiff took reasonable steps to maintain the  
4 confidentiality of her PII and relied on Defendant to keep their PII confidential  
5 and securely maintained, to use this information for employment purposes only,  
6 and to make only authorized disclosures of this information.  
7

8 14. As a result of the Data Breach, Plaintiff heeded Defendant's  
9 warnings and spent time dealing with the consequences of the Data Breach, which  
10 included time spent verifying the legitimacy of the Notice and self-monitoring  
11 their accounts and credit reports to ensure no fraudulent activity had occurred.  
12 This time has been lost forever and cannot be recaptured.  
13

14 15. Representative Plaintiff suffered actual injury in the form of  
15 damages to and diminution in the value of Representative Plaintiff's PII—a form  
16 of intangible property that Representative Plaintiff entrusted to Defendant, which  
17 was compromised in and because of the Data Breach.  
18

19 16. Representative Plaintiff suffered lost time, annoyance, interference,  
20 and inconvenience because of the Data Breach and have anxiety and increased  
21 concerns for the loss of privacy, as well as anxiety over the impact of  
22 unauthorized parties accessing, using, and selling Representative Plaintiff's PII.

23 17. Representative Plaintiff suffered imminent and impending injury  
24 arising from the substantially increased risk of fraud, identity theft, and misuse

1 resulting from their PII, in combination with her names, being placed in the hands  
2 of unauthorized third parties/criminals.

3 18. Representative Plaintiff has a continuing interest in ensuring that  
4 Representative Plaintiff's PII, which, upon information and belief, remains  
5 backed up in Defendant's possession, is protected and safeguarded from future  
6 breaches.  
7

### 8 *Plaintiff's Experiences*

9 19. Plaintiff Tamra Bacon is a customer of Defendant since 2017.

10 20. As a condition of maintaining accounts with Wells Fargo Bank,  
11 Plaintiff Tamra was required to provide her Private Information to Defendant,  
12 including her name, social security number, and financial information.  
13

14 21. At the time of the Data Breach, Defendant retained Plaintiff Tamra's  
15 Private Information in its system.

16 22. Plaintiff Tamra is very careful about sharing her sensitive Private  
17 Information. Plaintiff stores any documents containing her Private Information in  
18 a safe and secure location. She has never knowingly transmitted unencrypted  
19 sensitive Private Information over the internet or any other unsecured source.  
20 Plaintiff Tamra would not have entrusted her Private Information to Defendant  
21 had she known of Defendant's lax data security policies.  
22

23 23. As a result of the Data Breach, Plaintiff Tamra made reasonable  
24 efforts to mitigate the impact of the Data Breach, including researching and

1 verifying the legitimacy of the Data Breach upon discovering the breach,  
2 changing passwords and resecuring her own computer network, and contacting  
3 companies regarding suspicious activity on her accounts.

4           24. Plaintiff Tamra further spent time to freeze her credit as  
5 precaution—valuable time Plaintiff otherwise would have spent on other  
6 activities, including but not limited to work and/or recreation. This time has been  
7 lost forever and cannot be recaptured.

8           25. The Data Breach has caused Plaintiff Tamra to suffer fear, anxiety,  
9 and stress, which has been compounded by the fact that Defendant has still not  
10 fully informed her of key details about the Data Breach's occurrence.

11           26. As a result of the Data Breach, Plaintiff Tamra anticipates spending  
12 considerable time and money on an ongoing basis to try to mitigate and address  
13 harms caused by the Data Breach.

14           27. As a result of the Data Breach, Plaintiff Tamra is at a present risk  
15 and will continue to be at increased risk of identity theft and fraud for years to  
16 come.

17           28. Plaintiff Tamra has a continuing interest in ensuring that her Private  
18 Information, which, upon information and belief, remains backed up in  
19 Defendant's possession, is protected and safeguarded from future breaches.

20  
21  
22  
23  
24  
**DEFENDANT**

1 29. Defendant is a nationally chartered banking corporation doing  
2 business with principal headquarters located at 420 Montgomery Street San  
3 Francisco, CA 94104.

4 30. Defendant operates as a bank. Defendant offers online and mobile  
5 banking, home mortgage, loans and credit, investment and retirement, wealth  
6 management, and insurance services.

7  
8 31. The true names and capacities of persons or entities, whether  
9 individual, corporate, associate or otherwise, who may be responsible for some of  
10 the claims alleged here are currently unknown to Representative Plaintiffs.  
11 Representative Plaintiff will seek leave of court to amend this Complaint to  
12 reflect the true names and capacities of such responsible parties when their  
13 identities become known.  
14

### 15 16 **CLASS ACTION ALLEGATIONS**

17 32. Representative Plaintiff brings this action pursuant to the provisions  
18 of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure  
19 (“F.R.C.P.”) on behalf of Representative Plaintiff and the following  
20 classes/subclass(es) (collectively, the “Class(es)”):  
21

#### 22 **Nationwide Class:**

23 “All individuals within the United States of America whose  
24 PII was exposed to unauthorized third parties as a result of the  
data breach discovered by Defendant on or around July 2024.”



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
33. Excluded from the Classes 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, any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsel, and/or subdivisions, and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

11  
12  
34. In the alternative, Representative Plaintiff requests additional subclasses as necessary based on the types of PII that were compromised.

13  
14  
15  
16  
35. Representative Plaintiff reserves the right to amend the above Class definitions or to propose other subclasses in subsequent pleadings and motions for class certification.

17  
18  
19  
20  
36. This action has been brought and may properly be maintained as a class action under F.R.C.P. Rule 23 because there is a well-defined community of interest in the litigation and membership of the proposed Classes is readily ascertainable.

- 21  
22  
23  
24  
a. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy. The members of the Plaintiff Classes are so numerous that joinder of all members is impractical, if not impossible. Representative Plaintiff are informed and believe and, on that basis, allege that the total number of Class Members is in the thousands of

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

individuals. Membership in the Classes will be determined by analysis of Defendant's records.

b. Commonality: Representative Plaintiff and the Class Members share a community of interest in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

- 1) Whether Defendant had a legal duty to Representative Plaintiff and the Classes to exercise due care in collecting, storing, using and/or safeguarding their PII;
- 2) Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;
- 3) Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;
- 4) Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;
- 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
- 6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their PII had been compromised;
- 7) How and when Defendant actually learned of the Data Breach;
- 8) Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Representative Plaintiff and Class Members;
- 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff's and Class Members' PII;
- 11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

appropriate as a result of Defendant’s wrongful conduct;

12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant’s wrongful conduct.

c. Typicality: Representative Plaintiff’s claims are typical of the claims of the Plaintiff Classes. Representative Plaintiff and all members of the Plaintiff Classes sustained damages arising out of and caused by Defendant’s common course of conduct in violation of law, as alleged herein.

d. Adequacy of Representation: Representative Plaintiff in this class action is adequate representatives of each of the Plaintiff Classes in that Representative Plaintiff have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case and have retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the classes in their entirety. Representative Plaintiff anticipates no management difficulties in this litigation.

e. Superiority of Class Action: The damages suffered by individual Class Members are significant but may be small relative to each member’s enormous expense of individual litigation. This makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Even if Class Members could afford such individual litigation, the court system could not. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of other Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately. Individualized litigation increases the delay and expense to all parties and to the court system, presented by the case’s complex legal and factual issues. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale and comprehensive supervision by a single court.

S

1 37. Class certification is proper because the questions raised by this  
2 Complaint are of common or general interest affecting numerous persons, so it is  
3 impracticable to bring all Class Members before the Court.

4 38. This class action is also appropriate for certification because  
5 Defendant has acted or refused to act on grounds generally applicable to Class  
6 Members, thereby requiring the Court's imposition of uniform relief to ensure  
7 compatible standards of conduct toward the Class Members and making final  
8 injunctive relief appropriate concerning the Classes in their entirety.  
9 Defendant's policies and practices challenged herein apply to and affect Class  
10 Members uniformly. Representative Plaintiff's challenge of these policies and  
11 procedures hinges on Defendant's conduct concerning the Classes in their  
12 entirety, not on facts or law applicable only to Representative Plaintiff.  
13  
14

15 39. Unless a Class-wide injunction is issued, Defendant may continue  
16 failing to secure Class Members' PII properly, and Defendant may continue to act  
17 unlawfully, as set forth in this Complaint.

18 40. Further, Defendant has acted or refused to act on grounds generally  
19 applicable to the Classes and, accordingly, final injunctive or corresponding  
20 declaratory relief with regard to the Class Members as a whole is appropriate  
21 under F.R.C.P. Rule 23(b)(2).  
22

23 **COMMON FACTUAL ALLEGATIONS**

24 **The Data Breach**

1           41. During the Data Breach, one or more unauthorized third parties  
 2 accessed Class Members’ sensitive data including, but not limited to full names,  
 3 address, phone number, email address, dates of birth, driver’s license number,  
 4 bank account number(s), credit/debit card number, brokerage account number(s),  
 5 and/or loan/line of credit number(s) and Social Security numbers. Representative  
 6 Plaintiff was among the individuals whose data was accessed in the Data Breach.  
 7

8           42. According to Defendant, the Data Breach occurred when a former  
 9 employee “accessed, **and in some cases used**, customer information for  
 10 fraudulent purposes.”  
 11

12  
 13 **Defendant’s Failed Response to the Data Breach**

14           43. Not until months after it claims to have discovered the Data Breach  
 15 did Defendant begin sending the Notice to persons whose PII Defendant  
 16 confirmed was potentially compromised because of the Data Breach. The Notice  
 17 provided basic details of the Data Breach and Defendant’s recommended next  
 18 steps.  
 19

20           44. The Notice included, *inter alia*, the claims that Defendant had  
 21 learned of the Data Breach on or around July 2024, and had taken steps to  
 22 respond. But the Notice lacked sufficient information on how the breach  
 23 occurred, what safeguards have been taken since then to safeguard further attacks,  
 24 and/or where the information hacked exists today.

1           45. Upon information and belief, the unauthorized third-party gained  
2 access to Representative Plaintiff's and Class Members' PII with the intent of  
3 misusing the PII, including marketing and selling Representative Plaintiff's and  
4 Class Members' PII.

5  
6           46. Defendant had and continues to have obligations created by  
7 applicable federal and state law as set forth herein, reasonable industry standards,  
8 common law, and its own assurances and representations to keep Representative  
9 Plaintiff's and Class Members' PII confidential and to protect such PII from  
10 unauthorized access.

11  
12           47. Representative Plaintiff and Class Members were required to provide  
13 their PII to Defendant to receive services, and as part of providing services  
14 Defendant created, collected, and stored Representative Plaintiff's and Class  
15 Members' PII with the reasonable expectation and mutual understanding that  
16 Defendant would comply with its obligations to keep such information  
17 confidential and secure from unauthorized access.

18  
19           48. Despite this, even today, Representative Plaintiff and Class Members  
20 remain in the dark regarding what data was stolen, the particular malware used,  
21 and what steps are being taken to secure their PII in the future. Thus,  
22 Representative Plaintiff and Class Members are left to speculate as to where their  
23 PII ended up, who has used it, and for what potentially nefarious purposes.  
24 Indeed, they are left to further speculate as to the full impact of the Data Breach

1 and how Defendant intends to enhance its information security systems and  
2 monitoring capabilities to prevent further breaches.

3 49. Representative Plaintiff's and Class Members' PII may end up for  
4 sale on the dark web or fall into the hands of companies that will use the detailed  
5 PII for targeted marketing without Representative Plaintiff's and/or Class  
6 Members' approval. Either way, unauthorized individuals can now easily access  
7 Representative Plaintiff's and Class Members' PII.  
8

9 **Defendant Collected/Stored Representative Plaintiff's and Class Members'**  
10 **PII**

11 50. Defendant acquired, collected, stored, and assured reasonable  
12 security over Representative Plaintiff's and Class Members' PII.  
13

14 51. As a condition of its relationships with Representative Plaintiff and  
15 Class Members, Defendant required that Representative Plaintiff and Class  
16 Members entrust Defendant with highly sensitive and confidential PII. Defendant,  
17 in turn, stored that information on Defendant's system that was ultimately  
18 affected by the Data Breach.  
19

20 52. By obtaining, collecting, and storing Representative Plaintiff's and  
21 Class Members' PII, Defendant assumed legal and equitable duties over the PII  
22 and knew or should have known that it was thereafter responsible for protecting  
23 Representative Plaintiff's and Class Members' PII from unauthorized disclosure.  
24

1           53. Representative Plaintiff and Class Members have taken reasonable  
2 steps to maintain their PII's confidentiality. Representative Plaintiff and Class  
3 Members relied on Defendant to keep their PII confidential and securely  
4 maintained, to use this information for business and healthcare purposes only, and  
5 to make only authorized disclosures of this information.  
6

7           54. Defendant could have prevented the Data Breach, which began as  
8 early as May 2022, by properly securing and encrypting and/or more securely  
9 encrypting its servers, generally, as well as Representative Plaintiff's and Class  
10 Members' PII.

11           55. Defendant's negligence in safeguarding Representative Plaintiff's  
12 and Class Members' PII is exacerbated by repeated warnings and alerts directed  
13 at protecting and securing sensitive data, as evidenced by the trending data breach  
14 attacks in recent years.  
15

16           56. Data breaches such as the one experienced by Defendant have  
17 become so notorious that the Federal Bureau of Investigation ("FBI") and the  
18 U.S. Secret Service have issued a warning to potential targets so they are aware  
19 of, can prepare for, and hopefully ward off a potential attack.  
20

21           57. Due to the high-profile nature of these breaches and other breaches  
22 of its kind, Defendant was and/or certainly should have been on notice and aware  
23 of such attacks occurring in the healthcare industry and, therefore, should have  
24



1 assumed and adequately performed the duty of preparing for such an imminent  
2 attack.

3         58. And yet, despite the prevalence of public announcements of data  
4 breaches and data security compromises, Defendant failed to take appropriate  
5 steps to protect Representative Plaintiff's and Class Members' PII from being  
6 compromised.  
7

8  
9 **Defendant Had a Duty to Protect the Stolen Information**

10         59. In failing to adequately secure Representative Plaintiff's and Class  
11 Members' sensitive data, Defendant breached duties it owed Representative  
12 Plaintiff and Class Members under statutory and common law. Moreover,  
13 Representative Plaintiff and Class Members surrendered their highly sensitive  
14 personal data to Defendant under the implied condition that Defendant would  
15 keep it private and secure. Accordingly, Defendant also had an implied duty to  
16 safeguard their data, independent of any statute.  
17

18         60. Defendant was also prohibited by the Federal Trade Commission Act  
19 (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or  
20 practices in or affecting commerce." The Federal Trade Commission (the "FTC")  
21 has concluded that a company's failure to maintain reasonable and appropriate  
22 data security for consumers' sensitive personal information is an "unfair practice"  
23  
24

1 in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799  
2 F.3d 236 (3d Cir. 2015).

3           61. According to the FTC, the need for data security should be factored  
4 into all business decision-making. To that end, the FTC has issued numerous  
5 guidelines identifying best data security practices that businesses, such as  
6 Defendant, should employ to protect against the unlawful exposure of PII.  
7

8           62. In 2016, the FTC updated its publication, *Protecting Personal*  
9 *Information: A Guide for Business*, which established guidelines for fundamental  
10 data security principles and practices for business. The guidelines explain that  
11 companies should:  
12

- 13           a. protect the sensitive consumer information that they keep;
- 14           b. properly dispose of PII that is no longer needed;
- 15           c. encrypt information stored on computer networks;
- 16           d. understand their network's vulnerabilities; and
- 17           e. implement policies to correct security problems.

18           63. The guidelines also recommend that businesses watch for large  
19 amounts of data being transmitted from the system and have a response plan  
20 ready in the event of a breach.  
21

22           64. The FTC recommends that companies not maintain information  
23 longer than is necessary for authorization of a transaction, limit access to sensitive  
24 data, require complex passwords to be used on networks, use industry-tested

1 methods for security, monitor for suspicious activity on the network and verify  
2 that third-party service providers have implemented reasonable security measures.

3         65. The FTC has brought enforcement actions against businesses for  
4 failing to protect consumer data adequately and reasonably, treating the failure to  
5 employ reasonable and appropriate measures to protect against unauthorized  
6 access to confidential consumer data as an unfair act or practice prohibited by  
7 Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45.  
8 Orders resulting from these actions further clarify the measures businesses must  
9 take to meet their data security obligations.  
10

11         66. Defendant’s failure to employ reasonable and appropriate measures  
12 to protect against unauthorized access to consumers’ PII constitutes an unfair act  
13 or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.  
14

15         67. In addition to its obligations under federal and state laws, Defendant  
16 owed a duty to Representative Plaintiff and Class Members to exercise reasonable  
17 care in obtaining, retaining, securing, safeguarding, deleting, and protecting the  
18 PII in Defendant’s possession from being compromised, lost, stolen, accessed,  
19 and misused by unauthorized persons. Defendant owed a duty to Representative  
20 Plaintiff and Class Members to provide reasonable security, including consistency  
21 with industry standards and requirements, and to ensure that its computer  
22 systems, networks, and protocols adequately protected Representative Plaintiff’s  
23 and Class Members’ PII.  
24

1           68. Defendant owed a duty to Representative Plaintiff and Class  
2 Members to design, maintain, and test its computer systems, servers, and  
3 networks to ensure that all PII in its possession was adequately secured and  
4 protected.

5  
6           69. Defendant owed a duty to Representative Plaintiff and Class  
7 Members to create and implement reasonable data security practices and  
8 procedures to protect all PII in its possession, including not sharing information  
9 with other entities who maintain sub-standard data security systems.

10           70. Defendant owed a duty to Representative Plaintiff and Class  
11 Members to implement processes that would immediately detect a breach of its  
12 data security systems in a timely manner.

13  
14           71. Defendant owed a duty to Representative Plaintiff and Class  
15 Members to act upon data security warnings and alerts in a timely fashion.

16           72. Defendant owed a duty to Representative Plaintiff and Class  
17 Members to disclose if its computer systems and data security practices were  
18 inadequate to safeguard individuals' PII from theft, because such an inadequacy  
19 would be a material fact in the decision to entrust this PII to Defendant.

20  
21           73. Defendant owed a duty of care to Representative Plaintiff and Class  
22 Members because they were foreseeable and probable victims of any inadequate  
23 data security practices.

24

1           74. Defendant owed a duty to Representative Plaintiff and Class  
2 Members to encrypt and/or more reliably encrypt Representative Plaintiff's and  
3 Class Members' PII and monitor user behavior and activity to identify possible  
4 threats.

5  
6 **The Sensitive Information Stolen in the Data Breach is Highly Valuable**

7           75. It is well known that PII, including Social Security numbers and  
8 health records in particular, is a valuable commodity and a frequent, intentional  
9 target of cybercriminals. Companies that collect such information, including  
10 Defendant, are well aware of the risk of being targeted by cybercriminals.

11           76. Individuals place a high value not only on their PII but also on the  
12 privacy of that data. Identity theft causes severe negative consequences to its  
13 victims, as well as severe distress and hours of lost time trying to fight the impact  
14 of identity theft.

15           77. While the greater efficiency of electronic health records translates to  
16 cost savings for providers, it also comes with the risk of privacy breaches. PII is a  
17 valuable commodity for which a "cyber black market" exists where criminals  
18 openly post stolen Social Security numbers and other personal information on  
19 several underground internet websites. Unsurprisingly, the healthcare industry is  
20 at high risk and is acutely affected by cyberattacks, like the Data Breach here.

21           78. The high value of PII to criminals is evidenced by the prices they  
22 will pay for it through the dark web. For example, personal information can be  
23  
24

1 sold at a price ranging from \$40 to \$200, and bank details have a price range of  
2 \$50 to \$200.<sup>2</sup> Experian reports that a stolen credit or debit card number can sell  
3 for \$5 to \$110 on the dark web.<sup>3</sup> Criminals can also purchase access to entire  
4 company data breaches from \$999 to \$4,995.<sup>4</sup>

5  
6 79. Between 2005 and 2019, at least 249 million people were affected by  
7 healthcare data breaches.<sup>5</sup> Indeed, during 2019 alone, over 41 million healthcare  
8 records were exposed, stolen, or unlawfully disclosed in 505 data breaches.<sup>6</sup> In  
9 short, these sorts of data breaches are increasingly common, especially among  
10 healthcare systems, which account for 30.03 percent of overall health data  
11 breaches, according to cybersecurity firm Tenable.<sup>7</sup>

12  
13 80. These criminal activities have and will result in devastating financial  
14 and personal losses to Representative Plaintiff and Class Members. For example,  
15 it is believed that certain PII compromised in the 2017 Experian data breach was  
16 being used three years later by identity thieves to apply for COVID-19-related  
17 benefits in Oklahoma. Such fraud will be an omnipresent threat for  
18

---

19 <sup>2</sup> Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019,  
20 available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 24, 2023).

21 <sup>3</sup> *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017,  
22 available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed July 24, 2023).

23 <sup>4</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 24, 2023).

24 <sup>5</sup> <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/> (last accessed July 24, 2023).

<sup>6</sup> <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (last accessed July 24, 2023).

<sup>7</sup> <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/> (last accessed July 24, 2023).

1 Representative Plaintiff and Class Members for the rest of their lives. They will  
2 need to remain constantly vigilant.

3 81. The FTC defines identity theft as “a fraud committed or attempted  
4 using the identifying information of another person without authority.” The FTC  
5 describes “identifying information” as “any name or number that may be used,  
6 alone or in conjunction with any other information, to identify a specific person,”  
7 including, among other things, “[n]ame, Social Security number, date of birth,  
8 official State or government-issued driver’s license or identification number, alien  
9 registration number, government passport number, employer or taxpayer  
10 identification number.”  
11 identification number.”

12 82. Identity thieves can use PII, such as that of Representative Plaintiff  
13 and Class Members which Defendant failed to keep secure, to perpetrate various  
14 crimes that harm victims. For instance, identity thieves may commit various types  
15 of government fraud such as immigration fraud, obtaining a driver’s license or  
16 identification card in the victim’s name but with another’s picture, using the  
17 victim’s information to obtain government benefits, or filing a fraudulent tax  
18 return using the victim’s information to obtain a fraudulent refund.  
19

20 83. The ramifications of Defendant’s failure to secure Representative  
21 Plaintiff’s and Class Members’ PII are long-lasting and severe. Once PII is stolen,  
22 particularly identification numbers, fraudulent use of that information and  
23 damage to victims may continue for years. Indeed, the PII of Representative  
24

1 Plaintiff and Class Members was taken by hackers to engage in identity theft or to  
2 sell it to other criminals who will purchase the PII for that purpose. The  
3 fraudulent activity resulting from the Data Breach may not come to light for  
4 years.

5  
6 84. Individuals, like Representative Plaintiff and Class Members, are  
7 particularly concerned with protecting the privacy of their Social Security  
8 numbers, which are the key to stealing any person's identity and are likened to  
9 accessing DNA for hacker's purposes.

10 85. Data breach victims suffer long-term consequences when their Social  
11 Security numbers are taken and used by hackers. Even if they know their Social  
12 Security numbers are being misused, Representative Plaintiff and Class Members  
13 cannot obtain new numbers unless they become victims of Social Security  
14 misuse.

15  
16 86. The Social Security Administration has warned that "a new number  
17 probably won't solve all your problems. This is because other governmental  
18 agencies (such as the IRS and state motor vehicle agencies) and private  
19 businesses (such as banks and credit reporting companies) will have records  
20 under your old number. Along with other personal information, credit reporting  
21 companies use the number to identify your credit record. So, using a new number  
22  
23  
24



1 won't guarantee you a fresh start. This is especially true if your other personal  
2 information, such as your name and address, remains the same.”<sup>8</sup>

3 87. There may be a time lag between when harm occurs versus when it  
4 is discovered, and also between when PII is stolen and when it is used. According  
5 to the U.S. Government Accountability Office (“GAO”), which conducted a study  
6 regarding data breaches:  
7

8 [L]aw enforcement officials told us that in some cases, stolen data  
9 may be held for up to a year or more before being used to commit  
10 identity theft. Further, once stolen data have been sold or posted on  
the Web, fraudulent use of that information may continue for years.  
As a result, studies that attempt to measure the harm resulting from  
data breaches cannot necessarily rule out all future harm.<sup>9</sup>

11 88. And data breaches are preventable.<sup>10</sup> As Lucy Thompson wrote in  
12 the DATA BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data  
13 breaches that occurred could have been prevented by proper planning and the  
14 correct design and implementation of appropriate security solutions.”<sup>11</sup> She added  
15 that “[o]rganizations that collect, use, store, and share sensitive personal data  
16

---

17  
18  
19  
20 <sup>8</sup> *Identity Theft and Your Social Security Number*, SSA, No. 05-10064 (July 2021),  
<https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Apr. 18, 2023).

21 <sup>9</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at*:  
22 <http://www.gao.gov/new.items/d07737.pdf> (last accessed July 24, 2023).

23 <sup>10</sup> Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*  
24 *DATA BREACH AND ENCRYPTION HANDBOOK* (Lucy Thompson, ed., 2012)

<sup>11</sup> *Id.* at 17.

1 must accept responsibility for protecting the information and ensuring that it is  
2 not compromised....”<sup>12</sup>

3 89. Most of the reported data breaches are a result of lax security and the  
4 failure to create or enforce appropriate security policies, rules, and procedures.  
5 Appropriate information security controls, including encryption, must be  
6 implemented and enforced rigorously and disciplined so that a *data breach never*  
7 *occurs*.<sup>13</sup>

9 90. Here, Defendant knew of the importance of safeguarding PII and of  
10 the foreseeable consequences that would occur if Representative Plaintiff’s and  
11 Class Members’ PII was stolen, including the significant costs that would be  
12 placed on Representative Plaintiff and Class Members because of a breach of this  
13 magnitude. As detailed above, Defendant knew or should have known that the  
14 development and use of such protocols was necessary to fulfill its statutory and  
15 common law duties to Representative Plaintiff and Class Members. Therefore, its  
16 failure to do so is intentional, willful, reckless, and/or grossly negligent.

18 91. Furthermore, Defendant has offered only a two-year subscription for  
19 identity theft monitoring and identity theft protection through Experian  
20 IdentityWorks. Its limitation is inadequate when the victims will likely face many  
21 years of identity theft.  
22

---

23  
24 <sup>12</sup> *Id.* at 28.

<sup>13</sup> *Id.*

1           92. Moreover, Defendant's credit monitoring offer and advice to  
2 Representative Plaintiff and Class Members squarely place the burden on  
3 Representative Plaintiff and Class Members, rather than on Defendant, to monitor  
4 and report suspicious activities to law enforcement. In other words, Defendant  
5 expects Representative Plaintiff and Class Members to protect themselves from  
6 its tortious acts resulting from the Data Breach. Rather than automatically  
7 enrolling Representative Plaintiff and Class Members in credit monitoring  
8 services upon discovery of the Data Breach, Defendant merely sent instructions to  
9 Representative Plaintiff and Class Members about actions they could  
10 affirmatively take to protect themselves.  
11

12           93. These services are wholly inadequate as they fail to provide for the  
13 fact that victims of data breaches and other unauthorized disclosures commonly  
14 face multiple years of ongoing identity theft and financial fraud, and they entirely  
15 fail to provide any compensation for the unauthorized release and disclosure of  
16 Representative Plaintiff's and Class Members' PII.  
17

18           94. Defendant disregarded the rights of Representative Plaintiff and  
19 Class Members by, *inter alia*: (i) intentionally, willfully, recklessly and/or  
20 negligently failing to take adequate and reasonable measures to ensure that its  
21 network servers were protected against unauthorized intrusions, (ii) failing to  
22 disclose that it did not have adequate security protocols and training practices in  
23 place to safeguard Representative Plaintiff's and Class Members' PII, (iii) failing  
24

1 to take standard and reasonably available steps to prevent the Data Breach, (iv)  
2 concealing the existence and extent of the Data Breach for an unreasonable  
3 duration of time, and (v) failing to provide Representative Plaintiff and Class  
4 Members prompt and accurate notice of the Data Breach.

5  
6 **CAUSES OF ACTION**  
7 **COUNT ONE**  
8 **Negligence**  
9 **(On behalf of the Nationwide Class)**

10 95. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
11 Count with the same force and effect as though fully set forth herein.

12 96. At all times herein relevant, Defendant owed Representative Plaintiff  
13 and Class Members a duty of care, *inter alia*, to act with reasonable care to secure  
14 and safeguard their PII and to use commercially reasonable methods to do so.  
15 Defendant took on this obligation upon accepting and storing Representative  
16 Plaintiff’s and Class Members’ PII on its computer systems and networks.

- 17 97. Among these duties, Defendant was expected:
- 18 a. to exercise reasonable care in obtaining, retaining, securing,  
19 safeguarding, deleting and protecting the PII in its possession;
  - 20 b. to protect Representative Plaintiff’s and Class Members’ PII  
21 using reasonable and adequate security procedures and  
22 systems that were/are compliant with industry-standard  
23 practices;
  - 24 c. to implement processes to detect the Data Breach quickly and  
to act on warnings about data breaches timely; and
  - d. to promptly notify Representative Plaintiff and Class Members  
of any data breach, security incident or intrusion that affected  
or may have affected their PII.

98. Defendant knew or should have known that the PII was private and  
confidential and should be protected as private and confidential and, thus,

1 Defendant owed a duty of care to not subject Representative Plaintiff and Class  
2 Members to an unreasonable risk of harm because they were foreseeable and  
3 probable victims of any inadequate security practices.

4  
5 99. Defendant knew or should have known of the risks inherent in  
6 collecting and storing PII, the vulnerabilities of its data security systems and the  
7 importance of adequate security. Defendant knew or should have known about  
8 numerous well-publicized data breaches.

9  
10 100. Defendant knew or should have known that its data systems and  
11 networks did not adequately safeguard Representative Plaintiff's and Class  
12 Members' PII.

13  
14 101. Only Defendant was in the position to ensure that its systems and  
15 protocols were sufficient to protect the PII that Representative Plaintiff and Class  
16 Members had entrusted to it.

17  
18 102. Defendant breached its duties to Representative Plaintiff and Class  
19 Members by failing to provide fair, reasonable, or adequate computer systems and  
20 data security practices to safeguard their PII.

21  
22 103. Because Defendant knew that a breach of its systems could damage  
23 numerous individuals, including Representative Plaintiff and Class Members,  
24 Defendant had a duty to adequately protect its data systems and the PII stored  
thereon.

1           104. Representative Plaintiff’s and Class Members’ willingness to entrust  
2 Defendant with their PII was predicated on the understanding that Defendant  
3 would take adequate security precautions. Moreover, only Defendant could  
4 protect its systems and the PII it stored on them from attack. Thus, Defendant had  
5 a special relationship with Representative Plaintiff and Class Members.  
6

7           105. Defendant also had independent duties under state and federal laws  
8 that required Defendant to reasonably safeguard Representative Plaintiff’s and  
9 Class Members’ PII and promptly notify them about the Data Breach. These  
10 “independent duties” are untethered to any contract between Defendant,  
11 Representative Plaintiffs, and/or the remaining Class Members.  
12

13           106. Defendant breached its general duty of care to Representative  
14 Plaintiff and Class Members in, but not necessarily limited to, the following  
15 ways:

- 16           a. by failing to provide fair, reasonable and/or adequate  
17 computer systems and data security practices to safeguard  
Representative Plaintiff’s and Class Members’ PII;
- 18           b. by failing to timely and accurately disclose that Representative  
19 Plaintiff’s and Class Members’ PII had been improperly  
acquired or accessed;
- 20           c. by failing to adequately protect and safeguard PII by  
21 knowingly disregarding standard information security  
principles, despite obvious risks and by allowing unmonitored  
and unrestricted access to unsecured PII;
- 22           d. by failing to provide adequate supervision and oversight of the  
23 PII with which it was and is entrusted, in spite of the known  
risk and foreseeable likelihood of breach and misuse, which  
permitted an unknown third party to gather Representative  
24 Plaintiff’s and Class Members’ PII, misuse the PII and  
intentionally disclose it to others without consent;
- e. by failing to adequately train its employees not to store PII  
longer than absolutely necessary;

- 1 f. by failing to consistently enforce security policies aimed at  
protecting Representative Plaintiff's and Class Members' PII;
- 2 g. by failing to implement processes to quickly detect data  
3 breaches, security incidents or intrusions; and
- 4 h. by failing to encrypt Representative Plaintiff's and Class  
Members' PII and monitor user behavior and activity in order  
to identify possible threats.

5 107. Defendant's willful failure to abide by these duties was wrongful,  
6 reckless and/or grossly negligent in light of the foreseeable risks and known  
7 threats.

8  
9 108. As a proximate and foreseeable result of Defendant's grossly  
10 negligent conduct, Representative Plaintiff and Class Members have suffered  
11 damages and are at imminent risk of additional harm and damages (as alleged  
12 above).

13 109. The law further imposes an affirmative duty on Defendant to timely  
14 disclose the unauthorized access and theft of the PII to Representative Plaintiff  
15 and Class Members so that they could and/or still can take appropriate measures  
16 to mitigate damages, protect against adverse consequences, and thwart future  
17 misuse of their PII.

18  
19 110. Defendant breached its duty to notify Representative Plaintiff and  
20 Class Members of the unauthorized access by waiting roughly three months after  
21 learning of the Data Breach to notify Representative Plaintiff and Class Members  
22 and then by failing and continuing to fail to provide Representative Plaintiff and  
23 Class Members sufficient information regarding the breach. To date, Defendant  
24

1 has not provided sufficient information to Representative Plaintiff and Class  
2 Members regarding the extent of the unauthorized access and continues to breach  
3 its disclosure obligations to Representative Plaintiff and Class Members.

4  
5 111. Further, explicitly failing to provide timely and clear notification of  
6 the Data Breach to Representative Plaintiff and Class Members, Defendant  
7 prevented Representative Plaintiff and Class Members from taking meaningful,  
8 proactive steps to secure their PII and access their medical records and histories.

9  
10 112. There is a close causal connection between Defendant's failure to  
11 implement security measures to protect Representative Plaintiff's and Class  
12 Members' PII and the harm (or risk of imminent harm suffered) by  
13 Representative Plaintiff and Class Members. Representative Plaintiff's and Class  
14 Members' PII was accessed as the proximate result of Defendant's failure to  
15 exercise reasonable care in safeguarding such PII by adopting, implementing and  
16 maintaining appropriate security measures.

17  
18 113. Defendant's wrongful actions, inactions, and omissions constituted  
19 (and continue to constitute) common law negligence.

20  
21 114. The damages Representative Plaintiff and Class Members have  
22 suffered (as alleged above) and will continue to suffer were and are the direct and  
23 proximate result of Defendant's grossly negligent conduct.

24  
25 115. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair  
[...] practices in or affecting commerce," including, as interpreted and enforced



1 by the FTC, the unfair act or practice by businesses, such as Defendant, of failing  
2 to use reasonable measures to protect PII. The FTC publications and orders  
3 described above also form part of the basis of Defendant's duty in this regard.

4  
5 116. Defendant violated 15 U.S.C. § 45 by failing to use reasonable  
6 measures to protect PII and by not complying with applicable industry standards,  
7 as described in detail herein. Defendant's conduct was particularly unreasonable  
8 given the nature and amount of PII it obtained and stored and the foreseeable  
9 consequences of the immense damages that would result to Representative  
10 Plaintiff and Class Members.

11  
12 117. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per*  
13 *se*.

14 118. As a direct and proximate result of Defendant's negligence and  
15 negligence *per se*, Representative Plaintiff and Class Members have suffered and  
16 will continue to suffer injury, including but not limited to: (i) actual identity theft,  
17 (ii) the loss of the opportunity of how their PII is used, (iii) the compromise,  
18 publication, and/or theft of their PII, (iv) out-of-pocket expenses associated with  
19 the prevention, detection and recovery from identity theft, tax fraud, and/or  
20 unauthorized use of their PII, (v) lost opportunity costs associated with effort  
21 expended and the loss of productivity addressing and attempting to mitigate the  
22 actual and future consequences of the Data Breach, including but not limited to  
23 efforts spent researching how to prevent, detect, contest, and recover from  
24

1 embarrassment and identity theft, (vi) lost continuity in relation to their  
2 healthcare, (vii) the continued risk to their PII, which may remain in Defendant's  
3 possession and is subject to further unauthorized disclosures so long as Defendant  
4 fails to undertake appropriate and adequate measures to protect Representative  
5 Plaintiff's and Class Members' PII in its continued possession, and (viii) future  
6 costs in terms of time, effort, and money that will be expended to prevent, detect,  
7 contest, and repair the impact of the PII compromised as a result of the Data  
8 Breach for the remainder of the lives of Representative Plaintiff and Class  
9 Members.  
10

11           119. As a direct and proximate result of Defendant's negligence and  
12 negligence *per se*, Representative Plaintiff and Class Members have suffered and  
13 will continue to suffer other forms of injury and/or harm, including but not  
14 limited to anxiety, emotional distress, loss of privacy, and other economic and  
15 non-economic losses.  
16

17           120. Additionally, as a direct and proximate result of Defendant's  
18 negligence and negligence *per se*, Representative Plaintiff and Class Members  
19 have suffered and will continue to suffer the continued risks of exposure of their  
20 PII, which remains in Defendant's possession and is subject to further  
21 unauthorized disclosures so long as Defendant fails to undertake appropriate and  
22 adequate measures to protect PII in its continued possession.  
23  
24

**COUNT TWO**  
***Negligence Per Se***

**(On behalf of the Nationwide Class)**

1  
2       121. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
3 Count with the same force and effect as though fully set forth herein.

4       122. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45  
5 prohibits companies such as Defendant from “using any unfair method of  
6 competition or unfair or deceptive act or practice in or affecting commerce,”  
7 including failing to use reasonable measures to protect PII. In addition to the FTC  
8 Act, the agency also enforces other federal laws relating to consumers’ privacy  
9 and security. The FTC publications and orders described above also form part of  
10 the basis of Defendant’s duty in this regard.  
11

12       123. In addition to the FTC rules and regulations and state law, other  
13 states and jurisdictions where victims of the Data Breach are located require that  
14 Defendant protect PII from unauthorized access and disclosure and timely notify  
15 the victim of a data breach.  
16

17       124. Defendant violated FTC rules and regulations obligating companies  
18 to use reasonable measures to protect PII by failing to comply with applicable  
19 industry standards and by unduly delaying reasonable notice of the actual breach.  
20 Defendant’s conduct was particularly unreasonable given the nature and amount  
21 of PII it obtained and stored and the foreseeable consequences of a Data Breach  
22 and the exposure of Representative Plaintiff’s and Class members’ highly  
23 sensitive PII.  
24

1            125. Each of Defendant’s statutory violations of Section 5 of the FTC Act  
2 and other applicable statutes, rules and regulations, constitute negligence *per se*.

3            126. Representative Plaintiff and Class Members are within the category  
4 of persons the FTC Act were intended to protect.

5            127. The harm that occurred because of the Data Breach described herein  
6 is the type of harm the FTC Act was intended to guard against.

7            128. As a direct and proximate result of Defendant’s negligence *per se*,  
8 Representative Plaintiff and Class Members have been damaged as described  
9 herein, continue to suffer injuries as detailed above, are subject to the continued  
10 risk of exposure of their PII in Defendant’s possession and are entitled to  
11 damages in an amount to be proven at trial.  
12

13  
14                            **COUNT THREE**  
15                            **Breach of Confidence**  
16                            **(On behalf of the Nationwide Class)**

17            129. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
18 Count with the same force and effect as though fully set forth herein.

19            130. During Representative Plaintiff’s and Class Members’ interactions  
20 with Defendant, Defendant was fully aware of the confidential nature of the PII  
21 that Representative Plaintiff and Class Members provided to it.

22            131. As alleged herein and above, Defendant’s relationship with  
23 Representative Plaintiff and Class Members was governed by promises and  
24 expectations that Representative Plaintiff and Class Members’ PII would be

1 collected, stored, and protected in confidence, and would not be accessed by,  
2 acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by,  
3 released to, stolen by, used by, and/or viewed by unauthorized third parties.

4  
5 132. Representative Plaintiff and Class Members provided their  
6 respective PII to Defendant with the explicit and implicit understandings that  
7 Defendant would protect and not permit the PII to be accessed by, acquired by,  
8 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen  
9 by, used by, and/or viewed by unauthorized third parties.

10  
11 133. Representative Plaintiff and Class Members also provided their PII  
12 to Defendant with the explicit and implicit understanding that Defendant would  
13 take precautions to protect their PII from unauthorized access, acquisition,  
14 appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or  
15 viewing, such as following basic principles of protecting its networks and data  
16 systems.

17  
18 134. Defendant voluntarily received, in confidence, Representative  
19 Plaintiff's and Class Members' PII with the understanding that the PII would not  
20 be accessed by, acquired by, appropriated by, disclosed to, encumbered by,  
21 exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any  
22 unauthorized third parties.

23  
24 135. Due to Defendant's failure to prevent, detect and avoid the Data  
Breach from occurring by, *inter alia*, not following best information security

1 practices to secure Representative Plaintiff's and Class Members' PII,  
2 Representative Plaintiff's and Class Members' PII was accessed by, acquired by,  
3 appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen  
4 by, used by, and/or viewed by unauthorized third parties beyond Representative  
5 Plaintiff's and Class Members' confidence and without their express permission.  
6

7 136. As a direct and proximate cause of Defendant's actions and/or  
8 omissions, Representative Plaintiff and Class Members have suffered damages, as  
9 alleged herein.

10 137. But for Defendant's failure to maintain and protect Representative  
11 Plaintiff's and Class Members' PII in violation of the parties' understanding of  
12 confidence, their PII would not have been accessed by, acquired by, appropriated  
13 by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by,  
14 and/or viewed by unauthorized third parties. The Data Breach was the direct and  
15 legal cause of the misuse of Representative Plaintiff's and Class Members' PII  
16 and the resulting damages.  
17

18 138. The injury and harm Representative Plaintiff and Class Members  
19 suffered and will continue to suffer was the reasonably foreseeable result of  
20 Defendant's unauthorized misuse of Representative Plaintiff's and Class  
21 Members' PII. Defendant knew its data systems and protocols for accepting and  
22 securing Representative Plaintiff's and Class Members' PII had security and other  
23  
24

1 vulnerabilities that placed Representative Plaintiff's and Class Members' PII in  
2 jeopardy.

3           139. As a direct and proximate result of Defendant's breaches of  
4 confidence, Representative Plaintiff and Class Members have suffered and will  
5 continue to suffer injury, as alleged herein, including but not limited to: (i) actual  
6 identity theft, (ii) the compromise, publication, and/or theft of their PII, (iii) out-  
7 of-pocket expenses associated with the prevention, detection and recovery from  
8 identity theft and/or unauthorized use of their PII, (iv) lost opportunity costs  
9 associated with effort expended and the loss of productivity addressing and  
10 attempting to mitigate the actual and future consequences of the Data Breach,  
11 including but not limited to efforts spent researching how to prevent, detect,  
12 contest, and recover from identity theft, (v) the continued risk to their PII, which  
13 remains in Defendant's possession and is subject to further unauthorized  
14 disclosures so long as Defendant fails to undertake appropriate and adequate  
15 measures to protect Class Members' PII in its continued possession, (vi) future  
16 costs in terms of time, effort, and money that will be expended as result of the  
17 Data Breach for the remainder of the lives of Representative Plaintiff and Class  
18 Members, (vii) the diminished value of Representative Plaintiff's and Class  
19 Members' PII, and (viii) the diminished value of Defendant's services for which  
20 Representative Plaintiff and Class Members paid and received.  
21  
22  
23  
24

**COUNT FOUR**  
**Breach of Implied Contract**  
**(On behalf of the Nationwide Class)**

1  
2  
3       140. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
4 Count with the same force and effect as though fully set forth herein.

5       141. Through their course of conduct, Defendant, Representative Plaintiff  
6 and Class Members entered into implied contracts for Defendant to implement  
7 data security adequate to safeguard and protect the privacy of Representative  
8 Plaintiff's and Class Members' PII.

9  
10       142. Defendant required Representative Plaintiff and Class Members to  
11 provide and entrust their PII as a condition of obtaining Defendant's services.

12       143. Defendant solicited and invited Representative Plaintiff and Class  
13 Members to provide their PII as part of Defendant's regular business practices.  
14 Representative Plaintiff and Class Members accepted Defendant's offers and  
15 provided their PII to Defendant.

16  
17       144. As a condition of being Defendant's direct patients, Representative  
18 Plaintiff and Class Members provided and entrusted their PII to Defendant. In so  
19 doing, Representative Plaintiff and Class Members entered into implied contracts  
20 with Defendant by which Defendant agreed to safeguard and protect such non-  
21 public information, to keep such information secure and confidential and to  
22 timely and accurately notify Representative Plaintiff and Class Members if their  
23 data had been breached and compromised or stolen.  
24



1 145. A meeting of the minds occurred when Representative Plaintiff and  
2 Class Members agreed to, and did, provide their PII to Defendant, in exchange  
3 for, amongst other things, the protection of their PII.

4 146. Representative Plaintiff and Class Members fully performed their  
5 obligations under the implied contracts with Defendant.  
6

7 147. Defendant breached the implied contracts it made with  
8 Representative Plaintiff and Class Members by failing to safeguard and protect  
9 their PII and by failing to provide timely and accurate notice to them that their PII  
10 was compromised because of the Data Breach.

11 As a direct and proximate result of Defendant’s above-described breach of  
12 implied contract, Representative Plaintiff and Class Members have suffered and  
13 will continue to suffer: (i) ongoing, imminent and impending threat of identity  
14 theft crimes, fraud, and abuse, resulting in monetary loss and economic harm, (ii)  
15 actual identity theft crimes, fraud, and abuse, resulting in monetary loss and  
16 economic harm, (iii) loss of the confidentiality of the stolen confidential data, (iv)  
17 the illegal sale of the compromised data on the dark web, (v) lost work time, and  
18 (vi) other economic and non-economic harm.  
19  
20

21 **COUNT FIVE**  
22 **Breach of the Implied Covenant of Good Faith and Fair Dealing**  
23 **(On behalf of the Nationwide Class)**

24 148. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
Count with the same force and effect as though fully set forth herein.

1 149. Every contract in this State (California) has an implied covenant of  
2 good faith and fair dealing. This implied covenant is an independent duty and  
3 may be breached even when there is no breach of a contract's actual and/or  
4 express terms.

5  
6 150. Representative Plaintiff and Class Members have complied with and  
7 performed all conditions of their contracts with Defendant.

8 151. Defendant breached the implied covenant of good faith and fair  
9 dealing by failing to maintain adequate computer systems and data security  
10 practices to safeguard PII, failing to timely and accurately disclose the Data  
11 Breach to Representative Plaintiff and Class Members, and continued acceptance  
12 of PII and storage of other personal information after Defendant knew or should  
13 have known of the security vulnerabilities of the systems that were exploited in  
14 the Data Breach.

15  
16 152. Defendant acted in bad faith and/or with malicious motive in  
17 denying Representative Plaintiff and Class Members the full benefit of their  
18 bargains as originally intended by the parties, thereby causing them injury in an  
19 amount to be determined at trial.

20  
21 **COUNT SIX**  
**Breach of Fiduciary Duty**  
**(On behalf of the Nationwide Class)**

22 153. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
23 Count with the same force and effect as though fully set forth herein.

24

1           154. In light of the special relationship between Defendant and  
2 Representative Plaintiff and Class Members, whereby Defendant became the  
3 guardian of Representative Plaintiff’s and Class Members’ PII, Defendant  
4 became a fiduciary by its undertaking and guardianship of the PII to act primarily  
5 for Representative Plaintiff and Class Members, (i) for the safeguarding of  
6 Representative Plaintiff’s and Class Members’ PII, (ii) to timely notify  
7 Representative Plaintiff and Class Members of a data breach and disclosure, and  
8 (iii) to maintain complete and accurate records of what information (and where)  
9 Defendant did has and continues to store.  
10

11           155. Defendant has a fiduciary duty to act for the benefit of  
12 Representative Plaintiff and Class Members upon matters within the scope of its  
13 relationship with its customers’ patients and former patients—in particular, to  
14 keep their PII secure.  
15

16           156. Defendant breached its fiduciary duties to Representative Plaintiff  
17 and Class Members by failing to diligently discover, investigate, and give notice  
18 of the Data Breach in a reasonable and practicable period of time.  
19

20           157. Defendant breached its fiduciary duties to Representative Plaintiff  
21 and Class Members by failing to encrypt and otherwise protect the integrity of the  
22 systems containing Representative Plaintiff’s and Class Members’ PII.  
23  
24

1           158. Defendant breached its fiduciary duties to Representative Plaintiff  
2 and Class Members by failing to timely notify and/or warn Representative  
3 Plaintiff and Class Members of the Data Breach.

4           159. Defendant breached its fiduciary duties to Representative Plaintiff  
5 and Class Members by otherwise failing to safeguard Representative Plaintiff's  
6 and Class Members' PII.

7           160. As a direct and proximate result of Defendant's breaches of its  
8 fiduciary duties, Representative Plaintiff and Class Members have suffered and  
9 will continue to suffer injury, including but not limited to: (i) actual identity theft,  
10 (ii) the compromise, publication, and/or theft of their PII, (iii) out-of-pocket  
11 expenses associated with the prevention, detection, and recovery from identity  
12 theft and/or unauthorized use of their PII, (iv) lost opportunity costs associated  
13 with effort expended and the loss of productivity addressing and attempting to  
14 mitigate the actual and future consequences of the Data Breach, including but not  
15 limited to efforts spent researching how to prevent, contest, and recover from  
16 identity theft, (v) the continued risk to their PII, which remains in Defendant's  
17 possession and is subject to further unauthorized disclosures so long as Defendant  
18 fails to undertake appropriate and adequate measures to protect the PII in its  
19 continued possession, (vi) future costs in terms of time, effort, and money that  
20 will be expended as result of the Data Breach for the remainder of the lives of  
21  
22  
23  
24

1 Representative Plaintiff and Class Members, and (vii) the diminished value of  
2 Defendant's services they received.

3 161. As a direct and proximate result of Defendant's breach of its  
4 fiduciary duties, Representative Plaintiff and Class Members have suffered and  
5 will continue to suffer other forms of injury and/or harm, and other economic and  
6 non-economic losses.  
7

8 **COUNT SEVEN**  
9 **Unjust Enrichment**  
10 **(On behalf of the Nationwide Class)**

11 162. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
12 Count with the same force and effect as though fully set forth herein.

13 163. Upon information and belief, Defendant funds its data-security  
14 measures entirely from its general revenue, including payments made by or on  
15 behalf of Representative Plaintiff and Class Members.

16 164. As such, a portion of the payments made by or on behalf of  
17 Representative Plaintiff and Class Members is to be used to provide a reasonable  
18 level of data security, and the amount of each payment allocated to data security  
19 is known to Defendant.

20 165. Representative Plaintiff and Class Members conferred a monetary  
21 benefit to Defendant. Specifically, they purchased goods and services from  
22 Defendant and/or its agents and provided Defendant with their PII. In exchange,  
23 Representative Plaintiff and Class Members should have received from Defendant  
24

1 the goods and services that were the subject of the transaction and have their PII  
2 protected with adequate data security.

3 166. Defendant knew that Representative Plaintiff and Class Members  
4 conferred a benefit which Defendant accepted. Defendant profited from these  
5 transactions and used the PII of Representative Plaintiff and Class Members for  
6 business purposes.  
7

8 167. Defendant enriched itself by saving the costs it reasonably should  
9 have expended in data-security measures to secure Representative Plaintiff's and  
10 Class Members' PII. Instead of providing a reasonable level of security that  
11 would have prevented the hacking incident, Defendant instead calculated to  
12 increase its own profits at the expense of Representative Plaintiff and Class  
13 Members by utilizing cheaper, ineffective security measures. On the other hand,  
14 Representative Plaintiff and Class Members suffered as a direct and proximate  
15 result of Defendant's decision to prioritize its profits over the requisite security.  
16

17 168. Under the principles of equity and good conscience, Defendant  
18 should not be permitted to retain the money belonging to Representative Plaintiff  
19 and Class Members, because Defendant failed to implement appropriate data  
20 management and security measures mandated by industry standards.  
21

22 169. Defendant failed to secure Representative Plaintiff's and Class  
23 Members' PII and, therefore, did not provide full compensation for the benefit of  
24 Representative Plaintiff and Class Members.

1           170. Defendant acquired the PII through inequitable means in that it failed  
2 to disclose the inadequate security practices previously alleged.

3           171. If Representative Plaintiff and Class Members knew that Defendant  
4 had not reasonably secured their PII, they would not have agreed to provide their  
5 PII to Defendant.  
6

7           172. Representative Plaintiff and Class Members have no remedy at law.

8           173. As a direct and proximate result of Defendant's conduct,  
9 Representative Plaintiff and Class Members have suffered and will continue to  
10 suffer injury, including but not limited to: (i) actual identity theft, (ii) the loss of  
11 opportunity to determine how their PII is used, (iii) the compromise, publication,  
12 and/or theft of their PII, (iv) out-of-pocket expenses associated with the  
13 prevention, detection, and recovery from identity theft, and/or unauthorized use of  
14 their PII, (v) lost opportunity costs associated with efforts expended and the loss  
15 of productivity addressing and attempting to mitigate the actual and future  
16 consequences of the Data Breach, including but not limited to efforts spent  
17 researching how to prevent, detect, contest, and recover from identity theft, (vi)  
18 the continued risk to their PII, which remains in Defendant's possession and is  
19 subject to further unauthorized disclosures so long as Defendant fails to undertake  
20 appropriate and adequate measures to protect PII in its continued possession, and  
21 (vii) future costs in terms of time, effort and money that will be expended to  
22 prevent, detect, contest, and repair the impact of the PII compromised as a result  
23  
24

1 of the Data Breach for the remainder of the lives of Representative Plaintiff and  
2 Class Members.

3 174. As a direct and proximate result of Defendant's conduct,  
4 Representative Plaintiff and Class Members have suffered and will continue to  
5 suffer other forms of injury and/or harm.  
6

7 175. Defendant should be compelled to disgorge into a common fund or  
8 constructive trust, for the benefit of Representative Plaintiff and Class Members,  
9 proceeds that it unjustly received from them. In the alternative, Defendant should  
10 be compelled to refund the amounts that Representative Plaintiff and Class  
11 Members overpaid for Defendant's services.  
12

13 **COUNT EIGHT**  
14 **Declaratory Judgment**  
**(On behalf of the Nationwide Class)**

15 176. Each and every allegation of paragraphs 1 – 94 is incorporated in this  
16 Count with the same force and effect as though fully set forth herein.

17 177. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this  
18 Court is authorized to enter a judgment declaring the rights and legal relations of  
19 the parties and grant further necessary relief. Further, the Court has broad  
20 authority to restrain acts, such as here, that are tortious and violate the terms of  
21 the federal and state statutes described in this Complaint.  
22

23 178. An actual controversy has arisen after the Data Breach regarding  
24 Representative Plaintiff's and Class Members' PII and whether Defendant is



1 currently maintaining data security measures adequate to protect Representative  
2 Plaintiff and Class Members from further data breaches that compromise their  
3 PII. Representative Plaintiff allege that Defendant's data security measures  
4 remain inadequate. Defendant publicly denies these allegations. Furthermore,  
5 Representative Plaintiff continue to suffer injury due to the compromise of their  
6 PII and remain at imminent risk that further compromises of their PII will occur  
7 in the future. It is unknown what specific measures and changes Defendant has  
8 undertaken in response to the Data Breach.  
9

10           179. Representative Plaintiff and the Classes have an ongoing, actionable  
11 dispute arising out of Defendant's inadequate security measures, including: (i)  
12 Defendant's failure to encrypt Representative Plaintiff's and Class Members' PII,  
13 including Social Security numbers, while storing it in an Internet-accessible  
14 environment, and (ii) Defendant's failure to delete PII it has no reasonable need  
15 to maintain in an Internet-accessible environment, including the Social Security  
16 numbers of Representative Plaintiffs.  
17

18           180. Pursuant to its authority under the Declaratory Judgment Act, this  
19 Court should enter a judgment declaring, among other things, the following:  
20

- 21           a. Defendant owes a legal duty to secure the PII of  
22           Representative Plaintiff and Class Members;
- 23           b. Defendant continues to breach this legal duty by failing to  
24           employ reasonable measures to secure consumers' PII;

1 c. Defendant’s ongoing breaches of its legal duty continue to  
2 cause Representative Plaintiff harm.

3 181. This Court should also issue corresponding prospective injunctive  
4 relief requiring Defendant to employ adequate security protocols consistent with  
5 law, industry, and government regulatory standards to protect consumers’ PII.  
6 Specifically, this injunction should, among other things, direct Defendant to:

- 7 a. engage third-party auditors, consistent with industry standards,  
8 to test its systems for weakness and upgrade any such  
9 weakness found;
- 10 b. audit, test and train its data security personnel regarding any  
11 new or modified procedures and how to respond to a data  
12 breach;
- 13 c. regularly test its systems for security vulnerabilities, consistent  
14 with industry standards; and
- 15 d. implement an education and training program for appropriate  
16 employees regarding cybersecurity.

17 182. If an injunction is not issued, Representative Plaintiff will suffer  
18 irreparable injury, and lack an adequate legal remedy, in the event of another data  
19 breach at Defendant. The risk of another such breach is real, immediate, and  
20 substantial. If another breach at Defendant occurs, Representative Plaintiff will  
21 not have an adequate remedy at law because many of the resulting injuries are not  
22 readily quantified and they will be forced to bring multiple lawsuits to rectify the  
23 same conduct.

24



1           2. For an award of damages, including actual, nominal, and  
2 consequential damages, as allowed by law in an amount to be determined;

3           3. That the Court enjoin Defendant, ordering it to cease and desist from  
4 similar unlawful activities;

5           4. For equitable relief enjoining Defendant from engaging in the  
6 wrongful conduct complained of herein pertaining to the misuse and/or disclosure  
7 of Representative Plaintiff's and Class Members' PII, and from refusing to issue  
8 prompt, complete, and accurate disclosures to Representative Plaintiff and Class  
9 Members;  
10

11           5. For injunctive relief requested by Representative Plaintiffs, including  
12 but not limited to injunctive and other equitable relief as is necessary to protect  
13 the interests of Representative Plaintiff and Class Members, including but not  
14 limited to an Order:  
15

- 16           a. prohibiting Defendant from engaging in the wrongful and  
17 unlawful acts described herein;
- 18           b. requiring Defendant to protect, including through encryption,  
19 all data collected through the course of business in accordance  
20 with all applicable regulations, industry standards and federal,  
21 state or local laws;
- 22           c. requiring Defendant to delete and purge Representative  
23 Plaintiff's and Class Members' PII unless Defendant can  
24 provide to the Court reasonable justification for the retention  
and use of such information when weighed against the privacy  
interests of Representative Plaintiff and Class Members;
- d. requiring Defendant to implement and maintain a  
comprehensive Information Security Program designed to  
protect the confidentiality and integrity of Representative  
Plaintiff's and Class Members' PII;
- e. requiring Defendant to engage independent third-party  
security auditors and internal personnel to run automated

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

- f. prohibiting Defendant from maintaining Representative Plaintiff's and Class Members' PII on a cloud-based database;
- g. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- h. requiring Defendant to conduct regular database scanning and securing checks;
- i. 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 PII, as well as protecting the PII of Representative Plaintiff and Class Members;
- j. requiring Defendant to implement a system of tests to assess its respective 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;
- k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested and updated;
- l. requiring Defendant to meaningfully educate all Class Members about the threats they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law;

8. For all other Orders, findings and determinations identified and sought in this Complaint.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

**JURY DEMAND**

Representative Plaintiff, individually and on behalf of the Plaintiff Class(es) and/or Subclass(es), hereby demands a trial by jury for all issues triable by jury.

Dated: October 4, 2024



By: \_\_\_\_\_  
Daniel Srourian, Esq.  
**SROURIAN LAW FIRM, P.C.**  
3435 Wilshire Blvd., Suite 1710  
Los Angeles, California 90010  
Telephone: (213) 474-3800  
Facsimile: (213) 471-4160  
Email: [daniel@slfla.com](mailto:daniel@slfla.com)

*Counsel for Representative Plaintiff and  
the Proposed Class(es)*

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

TAMRA BACON, individually, and on behalf of all others similarly situated

(b) County of Residence of First Listed Plaintiff Wagoner, OK (EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

SROURIAN LAW FIRM, P.C. 468 N. Camden Dr., Suite 200 Beverly Hills, CA 90210

DEFENDANTS

WELLS FARGO BANK, N.A.

County of Residence of First Listed Defendant San Francisco County (IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- 1 U.S. Government Plaintiff 2 U.S. Government Defendant 3 Federal Question (U.S. Government Not a Party) 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

V. ORIGIN (Place an "X" in One Box Only)

- 1 Original Proceeding 2 Removed from State Court 3 Remanded from Appellate Court 4 Reinstated or Reopened 5 Transferred from Another District (specify) 6 Multidistrict Litigation-Transfer 8 Multidistrict Litigation-Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. § 1332(d)(2) and 15 U.S.C. § 45

Brief description of cause:

Negligence and Negligence Per Se, Breach of Confidence, Breach of Implied Contract, Breach of the Implied Covenant of Good Faith and Fair Dealing, Breach of Fiduciary Duty, Unjust Enrichment, Declaratory Judgment

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P.

DEMAND \$ 5,000,000.00

CHECK YES only if demanded in complaint: JURY DEMAND: X Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)

X SAN FRANCISCO/OAKLAND

SAN JOSE

EUREKA-MCKINLEYVILLE

DATE 10/04/2024

SIGNATURE OF ATTORNEY OF RECORD

/s/ Daniel Srourian

## INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

**Authority For Civil Cover Sheet.** The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
  - b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
  - c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
  - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
  - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
  - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
  - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
  - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
  - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
  - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
  - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
  - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.



AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

TAMRA BACON, individually, and on behalf of all others similarly situated

Plaintiff(s)

v.

WELLS FARGO BANK, N.A.,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) WELLS FARGO BANK, N.A. 420 Montgomery Street San Francisco, CA 94104

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Daniel Srourian, Esq. [SBN 285678] SROURIAN LAW FIRM, P.C. 468 N. Camden Dr., Suite 200 Beverly Hills, CA 90210 Telephone: (213) 474-3800 Fax: (213) 471-4160

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*: \_\_\_\_\_

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00 \_\_\_\_\_ .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc: