John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, CA 92101
Tel.: (858) 209-6941
jnelson@milberg.com
Attorney for Plaintiff

[Additional counsel listed on signature page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

CYNTHIA BEETS, on behalf of herself and all others similarly situated, Plaintiff, v. **WELLS FARGO BANK, N.A.,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Cynthia Beets ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Wells Fargo Bank, N.A. ("Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Wells Fargo Bank, N.A. for its failure to properly secure and safeguard Plaintiff's and other similarly situated Wells Fargo Bank, N.A. customers' name, address, date of birth, phone number, email address, social security number, driver's license number, bank account number(s), credit/ debit card number(s), brokerage account

number(s), and/or loan/line of credit number(s) (the "Private Information") from unauthorized access and exfiltration.

2. Wells Fargo Bank, N.A., based in San Francisco, California, is a prominent financial services company that serves tens of millions of customers nationwide.

3. On or about September 19, 2024, Wells Fargo Bank, N.A. filed official notice of a data breach incident with the Office of the Vermont Attorney General.[1] Subsequently, in or around early October 2024, it also sent out data breach email notices (the "Notice") to individuals whose information may have been compromised as a result of the hacking incident.

4. Based on the Vermont Attorney General notice and the Notice sent to impacted individuals, Wells Fargo Bank, N.A. only recently learned "that a former employee accessed, and in some cases used, customer information for fraudulent purposes" between May 2022 and March 2023 (the "Data Breach"). In response, the company launched an investigation in July of 2024 which revealed that Plaintiff's and putative Class Members' (defined below) highly sensitive Private Information was accessed during the Breach.

5. As a result of Defendant's delayed detection of, and response to, the Data Breach, Plaintiff and Class Members had no idea for many years that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

6. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, social security number, driver's license number, bank account number(s), credit/ debit card number(s), brokerage account number(s), and/or loan/line of credit number(s) that Wells Fargo Bank N.A. collected and maintained.

[1] See https://ago.vermont.gov/document/2024-09-19-wells-fargo-bank-data-breach-notice-consumers (last visited Oct. 8, 2024)

7. Armed with the Private Information accessed in the Data Breach, fraudsters can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. There has been no assurance offered by Wells Fargo Bank, N.A. that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

9. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff brings this class action lawsuit to address Wells Fargo Bank, N.A.'s inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiff and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access for fraudulent purposed.

11. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Wells Fargo Bank, N.A., and thus Wells Fargo Bank, N.A. was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

12. Upon information and belief, Wells Fargo Bank, N.A. and its employees failed to properly monitor and implement security practices with regard to the computer network and systems that housed the Private Information and allowed an employee to access and exfiltrate

Private Information without detection for years. Had Wells Fargo Bank, N.A. properly monitored its networks, limited access to essential and verifiable employees, and encrypted the Private Information, it would have discovered the Data Breach sooner or even prevented it altogether.

13. Plaintiff's and Class Members' identities are now at risk because of Wells Fargo Bank, N.A.'s negligent conduct as the Private Information that Wells Fargo Bank, N.A. collected and maintained is now in the hands of data thieves and other unauthorized third parties.

14. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

15. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

16. Plaintiff Cynthia Beets is, and at all times mentioned herein, was an individual citizen of the State of Tennessee.

17. Defendant Wells Fargo Bank, N.A. is a prominent financial services company with its principal place of business at 420 Montgomery Street, San Francisco, CA 94104.

III. JURISDICTION AND VENUE

18. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Wells Fargo Bank, N.A. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

19. This Court has jurisdiction over Wells Fargo Bank, N.A. because Wells Fargo Bank, N.A. operates in and/or is headquartered in this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Wells Fargo Bank, N.A. has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Wells Fargo Bank, N.A.'s Business and Collection of Plaintiff's and Class Members' Private Information

21. Wells Fargo Bank, N.A. is a premier financial services company. Founded in 1852, Wells Fargo Bank, N.A. is one of the largest financial institutions in the United States, serving millions of customers in 36 states. Wells Fargo Bank, N.A. employs more than 222,544 people and generates approximately $83 billion in annual revenue.

22. As a condition of receiving financial services, Wells Fargo Bank, N.A. requires that its customers entrust it with highly sensitive personal information. In the ordinary course of receiving service from Wells Fargo Bank, N.A., Plaintiff and Class Members were required to provide their Private Information to Defendant.

23. Wells Fargo Bank, N.A. uses this information, *inter alia*, for advertising, marketing, and business purposes.

24. In its "Notice of Data Breach," Wells Fargo Bank, N.A. states that "protecting our customers' information is a top priority."[2] In its privacy policy, Wells Fargo Bank, N.A. informs its customers "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards, secured files, and buildings."[3] Wells Fargo Bank, N.A. also states that "Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all

[2] *See* https://ago.vermont.gov/document/2024-09-19-wells-fargo-bank-data-breach-notice-consumers (last visited Oct. 8, 2024).

[3] *See* https://www.wellsfargo.com/assets/pdf/personal/privacy-security/us_consumer_privacy_notice_english.pdf (last visited Oct. 8, 2024).

Social Security numbers collected or retained by Wells Fargo Bank, N.A. in connection with customer, employee, or other relationships."[4]

25. Because of the highly sensitive and personal nature of the information Wells Fargo Bank, N.A. acquires and stores with respect to its customers, Wells Fargo Bank, N.A., upon information and belief, promises to, among other things: keep customers' Private Information private; comply with industry standards related to data security and the maintenance of its customers' Private Information; inform its customers of its legal duties relating to data security and comply with all federal and state laws protecting customers' Private Information; only use and release customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to customers if their Private Information is disclosed without authorization.

26. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Wells Fargo Bank, N.A. assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

27. Plaintiff and Class Members relied on Wells Fargo Bank, N.A. to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

B. The Data Breach and Wells Fargo Bank, N.A.'s Inadequate Notice to Plaintiff and Class Members

28. According to Defendant's Notice, it learned of unauthorized access to its computer systems in or around July 2024, with such unauthorized access having taken place between May 2022 and March 2023.

29. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including customers' name, address, date of birth, phone

[4] *Id.*

number, email address, social security number, driver's license number, bank account number(s), credit/ debit card number(s), brokerage account number(s), and/or loan/line of credit number(s).

30. On or about October 2024, roughly three months after Wells Fargo Bank, N.A. learned that the Class's Private Information was first accessed by an unauthorized employee, Wells Fargo Bank, N.A. finally began to notify customers that its investigation determined that their Private Information was accessed.

31. Wells Fargo Bank, N.A. delivered Data Breach Notification Letters to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "incident."

32. The notice letter then attached some pages entitled "Tips to Protect Your Personal Information," which listed generic steps that victims of data security incidents can take, such as getting a copy of a credit report or notifying law enforcement about suspicious financial account activity. Other than providing two years of credit monitoring that Plaintiff and Class Members would have to affirmatively sign up for and a call center number that victims could contact "with any questions," Wells Fargo Bank, N.A. offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Wells Fargo Bank, N.A. sent a similar generic letter to all individuals affected by the Data Breach.

C. Wells Fargo Bank, N.A. Failed to Comply with FTC Guidelines

33. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

34. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The

guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all network traffic for activity indicating someone is attempting unauthorized access to the system, watch for large amounts of data being transmitted from the system or downloaded, and have a response plan ready in the event of a breach.

35. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

37. As evidenced by the Data Breach, Wells Fargo Bank, N.A. failed to properly implement basic data security practices and controls to detect unauthorized internal access to its systems. Wells Fargo Bank, N.A. also failed to limit access to only necessary employees and to redact or encrypt Private Information. Wells Fargo Bank, N.A.'s failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

38. Wells Fargo Bank, N.A. was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Wells Fargo Bank, N.A. Failed to Comply with Industry Standards

39. Some industry best practices that should be implemented by businesses like Wells Fargo Bank, N.A. include but are not limited to educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

40. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

41. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Wells Fargo Bank, N.A. Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

42. In addition to its obligations under federal and state laws, Wells Fargo Bank, N.A. owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Wells Fargo Bank, N.A. owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members from both external and internal threats.

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

a. Failing to maintain an adequate data security system that would prevent or mitigate the risk of unauthorized internal access, including by limiting employee access and redacting or encrypting Private Information;

b. Failing to properly monitor its own data security systems for existing unauthorized access and unusual activity, including downloading or transfer of large amounts of data;

c. Failing to sufficiently train its employees regarding the proper handling of its customers Private Information;

d. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

e. Failing to adhere to industry standards for cybersecurity as discussed above; and

f. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

44. Wells Fargo Bank, N.A. negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing unfettered and undetectable access to its computer network and systems which contained unsecured and unencrypted Private Information.

45. Had Wells Fargo Bank, N.A. remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

46. Accordingly, Plaintiff's and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of

future harm that includes, but is not limited to, fraud and identity theft. Plaintiff and Class Members also lost the benefit of the bargain they made with Wells Fargo Bank, N.A.

F. Wells Fargo Bank, N.A. Should Have Known that Criminals Target Private Information to Carry Out Fraud and Identity Theft

47. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[5] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

48. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

49. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular personal privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity

[5] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Oct. 8, 2024).

Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

50. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

51. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [6] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[7]

52. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[8]

53. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[9] "Someone who has your SSN can use it to

---

[6] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.

[7] *Id.*

[8] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf

[9] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/

impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[10]

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

55. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[11]

56. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number

[10] *See* https://www.investopedia.com/terms/s/ssn.asp

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

derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target her in fraudulent schemes and identity theft attacks.")

57. Similarly, the California state government warns consumers that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[12]

58. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

59. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

60. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

61. One such example of this is the development of "Fullz" packages.

[12] *See* https://oag.ca.gov/idtheft/facts/your-ssn

62. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

63. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen Private Information are being misused, and that such misuse is fairly traceable to the Data Breach.

64. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[13] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

65. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's

[13] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Oct. 8, 2024).

information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

66. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

67. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[14] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

68. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[15] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[16]

69. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks

[14] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Oct. 8, 2024).

[15] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Oct. 8, 2024).

[16] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Oct. 8, 2024).

using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[17]

70. The Dark Web Price Index of 2022, published by PrivacyAffairs[18] shows how valuable just email addresses alone can be, even when not associated with a financial account:

2,400,000 million Canada email addresses	$100

71. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

72. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including Wells Fargo Bank, N.A. collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[19]

73. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[20]

[17] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Oct. 8, 2024).

[18] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Oct. 8, 2024).

[19] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Oct. 8, 2024).

[20] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

74. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

75. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

76. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

77. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[21]

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

78. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

[21] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Oct. 8, 2024).

79. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff's and Class Members' Damages

Plaintiff Cynthia Beets' Experience

80. When Plaintiff Beets first became a Wells Fargo Bank, N.A. customer, she was required to provide Wells Fargo Bank, N.A. with substantial amounts of her PII.

81. On or about October 2024, Plaintiff Beets received the Notice, which told her that the Private Information compromised in the Data Breach included her name, address, date of birth, phone number, email address, social security number, driver's license number, bank account number(s), credit/ debit card number(s), brokerage account number(s), and/or loan/line of credit number(s).

82. The Notice offered Plaintiff Beets only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff Beets will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

83. Plaintiff Beets suffered actual injury in the form of identity theft. She has already received multiple credit alerts notifying her that an unauthorized actor is attempting to open a line of credit using her personal information. In response, Plaintiff Beets placed a credit freeze on her account.

84. Plaintiff Beets suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

85. Plaintiff Beets would not have provided her Private Information to Defendant had Defendant timely disclosed that its systems lacked adequate computer and data security practices to safeguard its customers' personal information from theft, and that those systems were subject to a data breach.

86. Plaintiff Beets suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

87. Plaintiff Beets suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that Plaintiff Beets entrusted to Defendant for the purpose of receiving financial services from Defendant and which was compromised in, and as a result of, the Data Breach.

88. Plaintiff Beets suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

89. Plaintiff Beets has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches.

90. As a result of the Data Breach, Plaintiff Beets made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Beets has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

91. As a result of the Data Breach, Plaintiff Beets has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Beets is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

92. Plaintiff Beets also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Beets; (b) violation of her privacy rights; and (c) present,

imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

93. As a result of the Data Breach, Plaintiff Beets anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

94. In sum, Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

95. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services.

96. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

97. As a direct and proximate result of Wells Fargo Bank, N.A.'s actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card and debit card accounts opened in their names, and other forms of identity theft.

98. Further, as a direct and proximate result of Wells Fargo Bank, N.A.'s conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

99. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

100. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed

mosaic of Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

101. Plaintiff and Class Members also lost the benefit of the bargain they made with Wells Fargo Bank, N.A. Plaintiff and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to Wells Fargo Bank, N.A. was intended to be used by Wells Fargo Bank, N.A. to fund adequate security of Wells Fargo Bank, N.A.'s system and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive what they paid for.

102. Additionally, as a direct and proximate result of Wells Fargo Bank, N.A.'s conduct, Plaintiff and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

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

104. Additionally, Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[22] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[23]

[22] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Oct. 8, 2024).

[23] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Oct. 8, 2024).

105. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiff and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

106. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The contractual bargain entered into between Plaintiff and Defendant included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiff and Class Members did not get what they bargained for.

107. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

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

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

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

f. Contacting financial institutions and closing or modifying financial accounts;

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

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

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

108. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Wells Fargo Bank, N.A., is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

109. As a direct and proximate result of Wells Fargo Bank, N.A.'s actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

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

111. Specifically, Plaintiff proposes the following Nationwide Class (also referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

112. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

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

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

115. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of at least thousands of current and former Wells Fargo Bank, N.A. customers whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Wells Fargo Bank, N.A.'s records, Class Members' records, publication notice, self-identification, and other means.

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

a. Whether Wells Fargo Bank, N.A. engaged in the conduct alleged herein;

b. When Wells Fargo Bank, N.A. learned of the Data Breach;

c. Whether Wells Fargo Bank, N.A.'s response to the Data Breach was adequate;

d. Whether Wells Fargo Bank, N.A. unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether Wells Fargo Bank, N.A. failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Wells Fargo Bank, N.A.'s data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Wells Fargo Bank, N.A.'s data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Wells Fargo Bank, N.A. owed a duty to Class Members to safeguard their Private Information;

i. Whether Wells Fargo Bank, N.A. breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Wells Fargo Bank, N.A. had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether Wells Fargo Bank, N.A. breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Wells Fargo Bank, N.A. knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Wells Fargo Bank, N.A.'s misconduct;

o. Whether Wells Fargo Bank, N.A.'s conduct was negligent;

p. Whether Wells Fargo Bank, N.A.'s conduct was *per se* negligent;

q. Whether Wells Fargo Bank, N.A. was unjustly enriched;

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

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

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

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

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

120. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Wells Fargo Bank, N.A. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

122. Finally, all members of the proposed Class are readily ascertainable. Wells Fargo Bank, N.A. has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Wells Fargo Bank, N.A.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

123. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

124. Wells Fargo Bank, N.A. knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

125. Wells Fargo Bank, N.A.'s duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

126. Wells Fargo Bank, N.A. knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Wells Fargo Bank, N.A. was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

127. Wells Fargo Bank, N.A. owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Wells Fargo Bank, N.A.'s duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

128. Wells Fargo Bank, N.A.'s duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

129. Wells Fargo Bank, N.A.'s duty also arose because Defendant was bound by industry standards to protect its customers' confidential Private Information.

130. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Wells Fargo Bank, N.A. owed them a duty of care to not subject them to an unreasonable risk of harm.

131. Wells Fargo Bank, N.A., through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Wells Fargo Bank, N.A.'s possession.

132. Wells Fargo Bank, N.A., by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

133. Wells Fargo Bank, N.A., by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

134. Wells Fargo Bank, N.A. acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

135. Wells Fargo Bank, N.A. had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Wells Fargo Bank, N.A. with their Private Information was predicated on the understanding that Wells Fargo Bank, N.A. would take adequate security precautions. Moreover, only Wells Fargo Bank, N.A. had the ability to protect its systems (and the Private Information that it stored on them) from attack.

136. Wells Fargo Bank, N.A.'s breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and misused, as alleged herein.

137. As a result of Wells Fargo Bank, N.A.'s ongoing failure to notify Plaintiff and Class Members regarding exactly what Private Information has been compromised, Plaintiff and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

138. Wells Fargo Bank, N.A.'s breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

139. As a result of Wells Fargo Bank, N.A.'s negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

140. Wells Fargo Bank, N.A. also had independent duties under state laws that required it to reasonably safeguard Plaintiff's and Class Members' Private Information and promptly notify them about the Data Breach.

141. As a direct and proximate result of Wells Fargo Bank, N.A.'s negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

142. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

143. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

144. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Wells Fargo Bank, N.A. to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

145. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

146. This Count is pleaded in the alternative to Count II above.

147. Wells Fargo Bank, N.A. provides financial services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services from Defendant.

148. Through Defendant's sale of services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with Wells Fargo Bank, N.A.'s policies, practices, and applicable law.

149. Wells Fargo Bank, N.A.'s Privacy Policy memorialized the rights and obligations of Wells Fargo Bank, N.A. and its customers.

150. In the Privacy Policy, Wells Fargo Bank, N.A. commits to protecting the privacy and security of private information, especially Social Security numbers.

151. As consideration, Plaintiff and Class Members paid money to Wells Fargo Bank, N.A. and turned over valuable Private Information to Wells Fargo Bank, N.A. Accordingly, Plaintiff and Class Members bargained with Wells Fargo Bank, N.A. to securely maintain and store their Private Information.

152. Wells Fargo Bank, N.A. accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

153. In delivering their Private Information to Wells Fargo Bank, N.A. and paying for services, Plaintiff and Class Members intended and understood that Wells Fargo Bank, N.A. would adequately safeguard the Private Information as part of that service.

154. Defendant's implied promises to Plaintiff and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

155. Plaintiff and Class Members would not have entrusted their Private Information to Wells Fargo Bank, N.A. in the absence of such an implied contract.

156. Had Wells Fargo Bank, N.A. disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to Wells Fargo Bank, N.A.

157. Wells Fargo Bank, N.A. recognized that Plaintiff's and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

158. Wells Fargo Bank, N.A. violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

159. Plaintiff and Class Members have been damaged by Wells Fargo Bank, N.A.'s conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

160. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

161. This Count is pleaded in the alternative to Counts II and III above.

162. Plaintiff and Class Members conferred a benefit on Wells Fargo Bank, N.A. by turning over their Private Information to Defendant and by paying for services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

163. Upon information and belief, Wells Fargo Bank, N.A. funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiff and Class Members.

164. As such, a portion of the payments made by Plaintiff and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to Wells Fargo Bank, N.A.

165. Wells Fargo Bank, N.A. has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

166. Wells Fargo Bank, N.A. knew that Plaintiff and Class Members conferred a benefit upon it, which Wells Fargo Bank, N.A. accepted. Wells Fargo Bank, N.A. profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiff's and Class Members' Private Information and prevented the Data Breach.

167. If Plaintiff and Class Members had known that Wells Fargo Bank, N.A. had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

168. Due to Wells Fargo Bank, N.A.'s conduct alleged herein, it would be unjust and inequitable under the circumstances for Wells Fargo Bank, N.A. to be permitted to retain the benefit of its wrongful conduct.

169. As a direct and proximate result of Wells Fargo Bank, N.A.'s conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Wells Fargo Bank, N.A.'s possession and is subject to further unauthorized disclosures so long as Wells Fargo Bank, N.A. fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and

money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Wells Fargo Bank, N.A. to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Wells Fargo Bank, N.A. to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: October 11, 2024.

Respectfully submitted,

/s/ *John J. Nelson*
John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
402 W Broadway, Suite 1760
San Diego, CA 92101
Tel.: (858) 209-6941
jnelson@milberg.com

Tyler J. Bean (*pro hac vice* forthcoming)
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (646) 357-1732
E: tbean@sirillp.com

Attorneys for Plaintiff

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

CYNTHIA BEETS, on behalf of herself and all others similarly situated

(b) County of Residence of First Listed Plaintiff Out of state
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
John J. Nelson, Milberg Coleman Bryson Phillips Grossman, PLLC
402 W. Broadway, Suite 1760, San Diego, CA 92101
(858) 209-6941

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)*

unknown

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

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 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)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

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

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent–Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State 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)

Brief description of cause:
Data breach

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: ☒ 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) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 10/11/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ John J. Nelson

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.