UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

Dana Robbins and Alexander Hampel, individually and on behalf of themselves and all others similarly situated, Plaintiffs, v. Flagstar Bankcorp, Inc. and Flagstar Bank, FSB, Defendant.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Dana Robbins and Alexander Hampel ("Plaintiffs"), on behalf of themselves and all others similarly situated (the "Class Members"), bring this Class Action Complaint against Defendant Flagstar Bancorp, Inc. and Flagstar Bank, FSB ("Flagstar" or "Defendant"). The allegations in this Class Action Complaint ("Complaint") are based on the personal knowledge of Plaintiffs or upon information and belief and investigation of counsel.

NATURE OF CASE

1. This is a data breach class action brought on behalf of individuals whose sensitive personal information was stolen by cybercriminals in a massive cyberattack on Defendant's network between December 3 and December 4, 2021.

2. On June 2, 2022, or approximately six months after the breach took place, Defendant discovered that an unauthorized third party gained access to Defendant's network (the "Data Breach").[1] The Data Breach reportedly involved approximately 1,547,169 individuals.[2]

3. Information stolen in the Data Breach included individuals' sensitive personal identifying information, including name, Social Security number, account/loan number, and financial institution information ("Personal Identifying Information," "PII," or "Private Information").

4. Despite the breach occurring in December 2021, Defendant did not send notice of the data breach (the "Notice of Data Breach Letter") until June 17, 2022.

5. As a result of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of loss of value of their private and confidential information, theft and misuse of their Private Information, loss of the benefit of their

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml (last visited June 24, 2022).

[2] *Id.* The Regulatory Notification Update letter maintained on the Maine Attorney General's website indicated that 1,547,169 individuals were affected.

contractual bargain, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the attack, and mental anguish caused by the Data Breach.

6. Plaintiffs' and Class Members' Private Information—which was entrusted to Defendant, their officials, and agents—was compromised, unlawfully accessed, and stolen due to the Data Breach.

7. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Plaintiffs' and Class Members' Private Information that it collected and maintained.

8. Defendant maintained the Private Information in a reckless and negligent manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks of this type.

9. Upon information and belief, the mechanism of the cyber-attack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to Defendant, and Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition. In addition, Defendant and its employees and/or agents failed to properly monitor the computer network and systems that stored and maintained the Private Information. Had Defendant properly

monitored its systems, it would have been able to prevent the Data Breach or discover the intrusion sooner.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct, as the Private Information that Defendant collected and maintained is now in the hands of data thieves.

11. Armed with the Private Information accessed in the cyber-attack, data thieves 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' health information to target other phishing and hacking intrusions based on their individual health needs, 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.

12. As a further result of the Data Breach, Plaintiffs and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

13. Plaintiffs and Class Members have incurred and may also incur prospective out-of-pocket costs, *e.g.*, for purchasing credit monitoring services,

credit freezes, credit reports, or other protective measures to deter and detect identity theft.

14. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits, charges, and fees charged against their accounts; and deal with spam messages and e-mails received as a result of the Data Breach.

15. Plaintiffs and Class Members presently have and will continue to suffer from damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

16. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Data Breach.

17. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief, including improvements to Defendant' data security systems, future annual audits, and adequate credit monitoring and identity restoration services funded by Defendant.

18. Accordingly, Plaintiffs bring this action against Defendant seeking to redress Defendant's unlawful conduct.

PARTIES

19. Plaintiff Dana Robbins is a citizen of Indiana who currently and at all relevant times resided in Fort Wayne, Indiana. Plaintiff Dana Robbins experienced instances of fraud, including, but not limited, to fraudulent debit card purchases and a false unemployment application. Plaintiff Dana Robbins contacted Defendant's help line contained in the Notice of Data Breach Letter, wherein Defendant's customer service representative indicated that her PII was part of the Data Breach.

20. Plaintiff Alexander Hampel is a citizen of California who currently and at all times relevant times resided in Loleta, California. Plaintiff Alexander Hampel received a Notice of Data breach Letter, which informed him that his Social Security number, account/loan number, name, and financial institution information was disclosed.

21. Defendant Flagstar Bankcorp, Inc. is a corporation that was formed in Michigan and has its principal place of business in Troy, Michigan. Flagstar Bankcorp. Inc.'s corporate headquarters are located at 5151 Corporate Drive, Troy, Michigan 48098.

22. Defendant Flagstar Bank, FSB is a Michigan-based, federally chartered stock savings bank with its corporate headquarters located at 5151 Corporate Drive, Troy, Michigan 48098.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

24. This Court has personal jurisdiction over Defendant as Defendant's principal places of business are located within this District.

25. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District; Defendant resides within this judicial district; and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

26. Upon information and belief, Defendant obtains Plaintiffs' and Class Members' PII to provide its services. Notably, Defendant's Privacy Policy promises

to protect Plaintiffs' and Class Members' PII—"[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 and secured files and buildings." [3]

27. Defendant experienced a cyber incident that involved unauthorized access to its network. After an investigation, on June 2, 2022, Defendant discovered that an unauthorized third party accessed Defendant's network and obtained files containing Social Security numbers, account/loan number, name, and financial institution name.

28. In the course of collecting PII, Defendant promised to provide confidentiality and adequate security for customer data through their applicable privacy policy and through other disclosures.

The Data Breach

29. On or about June 2, 2022, Defendant confirmed that an unauthorized third party gained access to Defendant's network on or around December 3, 2021 and December 4, 2021, and impacted files containing Plaintiffs' and Class Members' PII, including, but not limited to, Social Security numbers, account/loan number, name, and financial institution name.

[3] https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf (last viewed: June 24, 2022).

30. Despite the breach taking place in December 2021, Defendant did not notify Plaintiffs and Class Members until June 17, 2022.

31. Defendant admits that Plaintiffs' and Class Members' Private Information was "compromised" in the Data Breach.

32. On information and belief, Defendant failed to encrypt the PII stored on their systems, evidenced by the fact that hackers were able to steal the Private Information in a useable form.

33. Defendant acknowledges that Plaintiffs and Class Members face a substantial and present risk of identity theft because Defendant "secured services of Kroll to provide identity monitoring at no cost…for two years."

34. Based on Defendant's statement to Plaintiff Robbins, which informed Plaintiff that her Private Information was included in the Data Breach.

35. Based on the Notice of Data Breach letter received by Plaintiff Hampel, which informed Plaintiffs and Class Members that their Private Information was obtained from Defendant's network and computer systems, Plaintiff reasonably believes that his Private Information was stolen from Defendant's network and systems (and subsequently sold) as a result of the Data Breach.

36. Further, the removal of the Private Information from Defendant's system demonstrates that this cyberattack was targeted.

37. Additionally, though Plaintiffs and Class Members have an interest in ensuring that their information remains protected, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures taken to ensure a breach does not occur again have not been shared with regulators, Plaintiffs, or Class Members.

Defendant Was Aware of the Data Breach Risks

38. Defendant had obligations created by contract, industry standards, and common law to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

39. Plaintiffs and Class Members had a reasonable expectation that Defendant would comply with their obligations to employ reasonable care to keep PII confidential and secure from unauthorized access.

40. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the Data Breach.

41. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant

risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

42. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity thieves use the stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.

43. The PII of Plaintiffs and Class Members was taken by cyber criminals for the very purpose of engaging in identity theft, or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

44. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers and health information, and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members a result of a breach.

45. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. They are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

46. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Defendant Failed to Comply with FTC Guidelines

47. The FTC has promulgated numerous guides for businesses that 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.

48. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security 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 networks' 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 incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

49. The FTC further recommends that companies not maintain 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 for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, 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 Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

51. Defendant failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered;

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing;

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users;

d. Configure firewalls to block access to known malicious IP addresses;

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system;

f. Set anti-virus and anti-malware programs to conduct regular scans automatically;

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary;

h. Configure access controls—including file, directory, and network share permissions— with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares;

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications;

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware

locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder;

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used;

l. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy;

m. Execute operating system environments or specific programs in a virtualized environment; and

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

53. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

1. **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.

2. **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization’s website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).

3. **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

4. **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it.

5. **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

6. **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

7. **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[4]

54. Defendant was at all times fully aware of their obligation to protect the PII and PHI of those whose information was entrusted to it. Defendant was also aware of the significant repercussions that would result from their failure to do so.

Defendant Failed to Comply with Industry Standards

[4] https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Jan. 6, 2022).

55. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

56. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness. These frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

57. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach.

Defendant's Breach

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

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

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor their data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

59. As the result of computer systems in dire need of security upgrading and inadequate procedures for handling cybersecurity threats, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

60. Accordingly, as outlined below, Plaintiffs and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

61. Defendant was well aware that the Private Information they collect is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

62. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[5]

[5] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Jan. 6, 2022) ("GAO Report").

63. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it.

64. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims and take over victims' identities in order to engage in illegal financial transactions under the victims' names. 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 otherwise harass or track the victim.

65. For example, armed with just a name and date of birth, a data thief can use 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.

66. 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.

67. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud

alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[6]

68. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

69. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

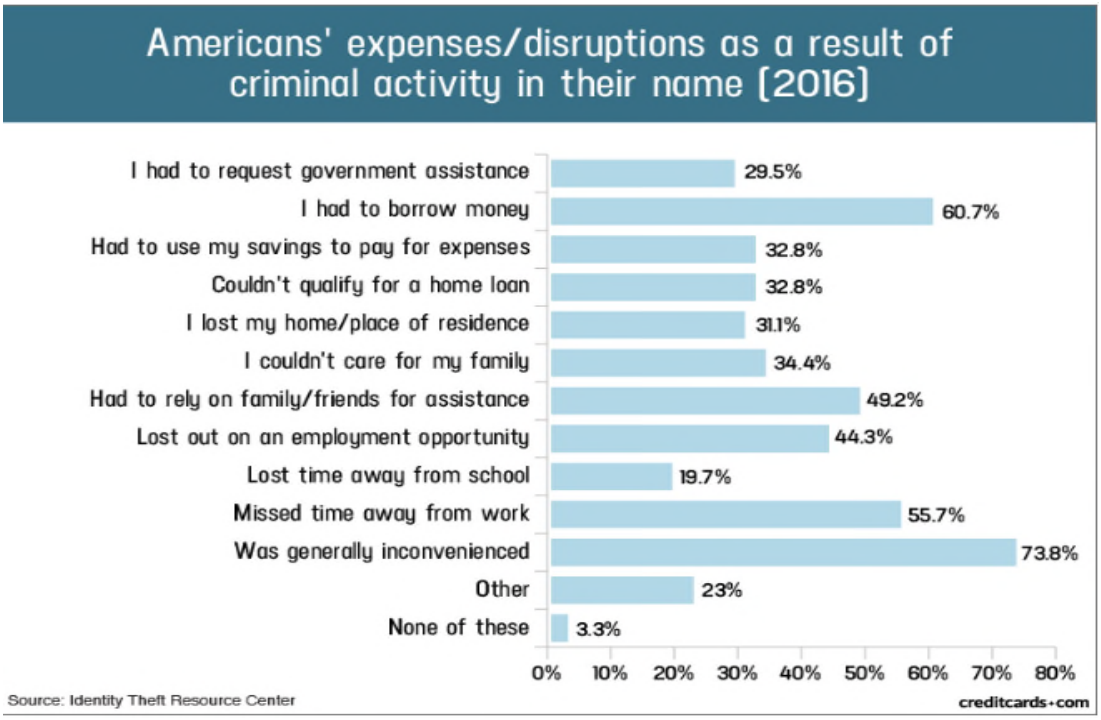
70. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[7]

---

[6] *See* https://www.identitytheft.gov/Steps (last visited Jan. 6, 2022).

[7] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020), available at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Jan. 6, 2022).



72. What's more, theft of Private Information is also gravely serious. PII is a valuable property right.[8]

73. The value of PII is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

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

74. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

75. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at 29.

76. Private Information, health information, and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

77. There is a strong probability that entire batches of stolen information have been dumped on the black market and will continue to be dumped on the black market, meaning Plaintiffs and Class Members are at a substantial and immediate present risk of fraud and identity theft that will continue for many years.

78. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

79. Sensitive Private Information can sell for as much as $363 according to the Infosec Institute.

80. PII is particularly valuable because criminals can use it to target victims with frauds and scams.

81. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

82. The PII of consumers like Plaintiffs and Class Members 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, personal information can be sold at a price ranging from $40 to $200.

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

84. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make

it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.

85. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

86. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

87. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[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."[9]

88. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable

[9] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, available at: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Jan. 6, 2022).

information and Social Security Numbers are worth more than 10x on the black market."[10]

89. At all relevant times, Defendant knew or reasonably should have known these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached, and they should have strengthened their data systems accordingly. Defendant were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

90. Plaintiffs and Class Members have been damaged by the compromise of their PII in the Data Breach.

91. Plaintiffs and Class Members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

92. Plaintiffs and Class Members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegality based on their PII as potential fraudsters could use that

[10] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, available at: http://www.itworld.com/article/2880960/anthem-hack-personal-(last visited Jan. 6, 2022).

information to target such schemes more effectively to Plaintiffs and Class Members.

93. Plaintiffs 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.

94. Plaintiffs 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 data breach cases.

95. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

96. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses 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.

97. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents

containing personal and financial information is not accessible online and that access to such data is password protected.

98. Further, as a result of Defendant's conduct, Plaintiffs and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

99. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and are at an increased risk of future harm.

PLAINTIFFS'S EXPERIENCE

Plaintiff Robbins' Experience

100. Plaintiff Robbins' PII and other confidential information was entrusted to Defendant and Plaintiff had a reasonable expectation that Defendant would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her PII.

101. Plaintiff has been forced to spend time dealing with and responding to the direct consequences of the Data Breach, which include spending time on telephone calls, researching the Data Breach, exploring credit monitoring and

identity theft insurance options, and self-monitoring her accounts. This is time that has been lost forever and cannot be recaptured.

102. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of her PII – a form of intangible property that was entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

103. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has anxiety and increased concerns due to the loss of her privacy and the substantial risk of fraud and identity theft that she now faces.

104. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of her PII resulting from the compromise of her PII, especially her Social Security number, in combination with her name, address, and other information, which PII is now in the hands of cyber criminals and other unauthorized third parties.

105. Knowing that thieves stole her PII, including her Social Security number and other PII that she was required to provide to Defendant, and knowing that her PII will likely be sold on the dark web, has caused Plaintiff great anxiety.

106. Additionally, Plaintiff does not recall having been involved in any other data breaches in which her highly confidential PII, such as Social Security Number

was compromised.

107. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief remains in the possession of Defendant, is protected and safeguarded from future data breaches.

108. As a result of the Data Breach, Plaintiff has been the victim of false debit card charges and had to obtain a new debit card. Put simply, Plaintiffs' debit card and associated accounts have been compromised due to Defendant's negligence.

109. As a result of the Data Breach, Plaintiff was informed that an individual filed a false unemployment claim on her behalf.

110. As a result of the Data Breach, Plaintiff is presently and will continue to be at a heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

Plaintiff Alexander Hampel

111. Plaintiff Hampel's PII and other confidential information was entrusted to Defendant and Plaintiff had a reasonable expectation that Defendant would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to her PII.

112. Plaintiff has been forced to spend time dealing with and responding to

the direct consequences of the Data Breach, which include spending time on the telephone calls, researching the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This is time that has been lost forever and cannot be recaptured.

113. Plaintiff has suffered actual injury in the form of damages to, and diminution in, the value of his PII – a form of intangible property that was entrusted to Defendant. This PII was compromised in, and has been diminished as a result of, the Data Breach.

114. Plaintiff has also suffered actual injury in the forms of lost time and opportunity costs, annoyance, interference, and inconvenience as a result of the Data Breach, and has increased concerns due to the loss of his privacy and the substantial risk of fraud and identity theft that he now faces.

115. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse of his PII resulting from the compromise of his PII, especially his Social Security number, in combination with his name, address, and other information, which PII is now in the hands of cyber criminals and other unauthorized third parties.

116. Knowing that thieves stole his PII, including his Social Security number and other PII that he was required to provide to Defendant, and knowing that his PII will likely be sold on the dark web, has caused Plaintiff great anxiety.

117. Additionally, Plaintiff does not recall having been involved in any other data breaches in which his highly confidential PII, such as Social Security Number was compromised.

118. Plaintiff has a continuing interest in ensuring that his PII, which upon information and belief remains in the possession of Defendant, is protected and safeguarded from future data breaches.

119. As a result of the Data Breach, Plaintiff is presently and will continue to be at a heightened risk for financial fraud, identity theft, other forms of fraud, and the attendant damages, for years to come.

CLASS ALLEGATIONS

120. Plaintiffs bring this nationwide class action pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), individually and on behalf of all members of the Class:

> All natural persons residing in the United States whose PII was compromised in the Data Breach initially discovered by Defendant on or about June 2, 2022 (the "Nationwide Class").

121. In addition, Plaintiff Hampel brings a class action pursuant to California's Class Action Mechanism (Cal. Civ., § 382) for the following Subclass defined as:

> California Subclass: All individuals and entities residing or have resided in California whose PII was compromised in the Data Breach on or about June 2, 2022 (the "California Subclass").

122. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

123. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

124. **Numerosity**. The Class is so numerous that joinder of all members is impracticable. The Class includes hundreds of thousands of individuals whose personal data was compromised by the Data Breach. The exact number of Class Members is in the possession and control of Defendant and will be ascertainable through discovery, but is believed, based on Defendant's disclosures, to exceed 1,500,000.

125. **Commonality.** There are numerous questions of law and fact common to Plaintiffs and the Class that predominate over any questions that may affect only individual Class Members, including, without limitation:

a. Whether Defendant unlawfully maintained, lost or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

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

e. Whether Defendant owed a duty to Class Members to safeguard their PII;

f. W

g. Whether Defendant breached duties to Class Members to safeguard their PII;

h. W

i. Whether cyber criminals obtained Class Members' PII in the Data Breach;

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

k. Whether Defendant owed a duty to provide Plaintiffs and Class Members notice of this Data Breach, and whether Defendant breached that duty to provide timely notice;

l. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

m. Whether Defendant violated California's UCL §17200 – Unlawful Business Practice;

n. Whether Defendant violated California's UCL §17200 – Unfair Business Practice;

o. Whether Defendant's conduct was negligent;

p. Whether Defendant's conduct violated federal law;

q. Whether Defendant's conduct violated state law; and

r. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

126. Typicality. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class Members, had their personal data compromised, breached, and stolen in the Data Breach. Plaintiffs and all Class Members were injured through the uniform misconduct of Defendant, described throughout this Complaint, and assert the same claims for relief.

127. Adequacy. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs retained counsel who are experienced in Class action and complex litigation. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other Class Members.

128. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendant's conduct

and/or inaction. Plaintiffs knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

129. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member. Specifically, injunctive relief could be entered in multiple cases, but the ordered relief may vary, causing Defendant to have to choose between differing means of upgrading their data security infrastructure and choosing the court order with which to comply. Class action status is also warranted because prosecution of separate actions by Class Members would create the risk of adjudications with respect to individual Class Members that, as a practical matter, would be dispositive of the interests of other members not parties to this action, or that would substantially impair or impede their ability to protect their interests.

130. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

131. Likewise, particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether Plaintiffs and Class Members are entitled to actual damages, or injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

132. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

133. Defendant owed to Plaintiffs and Class Members a duty of reasonable care to protect Plaintiffs' and the Class Members' data from the foreseeable threat of theft during a Data Breach. This duty arose from several sources.

134. Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

135. The legal duties owed by Defendant to Plaintiffs and Class Members include, but are not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and Class Members in Defendant's possession;

b. To protect the PII of Plaintiffs and Class Members in Defendant's possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class Members of the Data Breach.

136. Defendant's duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the Federal Trade Commission, the unfair practices by companies such as Defendant of failing to use reasonable measures to protect PII.

137. Various FTC publications and data security breach orders further form the basis of Defendant's duty. Plaintiffs and Class Members are consumers under the FTC Act. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

138. Defendant breached their duties to Plaintiffs and Class Members. Defendant knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

139. Defendant knew or should have known that their security practices did not adequately safeguard the PII of Plaintiffs and Class Members.

140. Through Defendant's acts and omissions described in this Complaint, including Defendant's failure to provide adequate security and its failure to protect the PII and PHI of Plaintiffs and Class Members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendant unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members during the time it was within Defendant's possession and control.

141. Defendant breached the duties they owe to Plaintiffs and Class Members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to Plaintiffs and Class Members that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

142. Due to Defendant's conduct, Plaintiffs and Class Members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against them immediately and for years to come.

143. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219.00 to $358.00 per year.

144. As a result of Defendant's negligence, Plaintiffs and Class Members suffered injuries that may include:

(i) actual identity theft;

(ii) the lost or diminished value of PII;

(iii) the compromise, publication, and/or theft of PII;

(iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

(vi) the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession;

(vii) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, including ongoing credit monitoring.

145. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiffs and Class Members suffered was the direct and proximate result of Defendant's negligent conduct.

SECOND CLAIM
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class)

146. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 129.

147. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

148. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry

standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Class Members due to the valuable nature of the PII at issue in this case—including Social Security numbers.

149. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

150. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

151. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

152. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to:

i. actual identity theft;

ii. the lost or diminished value of PII;

iii. the compromise, publication, and/or theft of PII and PHI;

iv. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

v. lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account;

vi. costs associated with placing freezes on credit reports;

vii. the continued risk to their PII, which may remain for sale on the dark web and is in Defendant's possession and subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession;

viii. future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members, including ongoing credit monitoring.

153. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM
Unjust Enrichment
(On behalf of Plaintiffs and the Nationwide Class)

154. Plaintiffs and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

155. Defendant benefited from receiving Plaintiffs' and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

156. Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

157. Plaintiffs and Class Members conferred a monetary benefit upon Defendant in the form of providing their Private Information to Defendant and Plaintiffs' and Class Members' employers conferred a monetary benefit by purchasing loan services. In connection thereto, Plaintiffs and Class Members and/or their employers provided Private Information to Defendant with the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures. Specifically, Plaintiffs and Class Members were required to provide their Private Information. In exchange, Plaintiffs and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

158. Defendant knew Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

159. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members.

160. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

161. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

162. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

163. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

FOURTH CLAIM
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the California Subclass)

164. Plaintiffs and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

165. By reason of the conduct alleged herein, Defendant engaged in unlawful "business practices" within the meaning of the UCL.

166. Defendant stored patient and employee data of Plaintiffs and the Class Members in its computer systems. Defendant falsely represented to Plaintiffs and the Class Members that their Private Information was secure and would remain private.

167. Defendant knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiffs' and the Class Member's Private Information a secure and prevented the loss or misuse of that Private Information.

168. Even without these misrepresentations, Plaintiffs and Class Members were entitled to assume, and did assume Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any time that Plaintiffs' Private Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose. Defendant violated the UCL by misrepresenting, both by affirmative conduct and by omission, the safety of its computer systems, specifically the security thereof, and its ability to

safely store Plaintiffs' and Class Members' Private Information. Defendant also violated the UCL by failing to implement reasonable and appropriate security measures or follow industry standards for data security, failing to comply with its own posted privacy policies, and by failing to immediately notify Plaintiffs and Class Members of the Data Breach. If Defendant had complied with these legal requirements, Plaintiffs and Class Members would not have suffered the damages related to the Data Breach, and consequently from, Defendant's failure to timely notify Plaintiffs and the Class Members of the Data Breach.

169. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

170. Plaintiffs and Class Members suffered injury in fact and lost money or property as the result of Defendant's unlawful business practices. In particular, Plaintiffs and Class Members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and Class Members have also suffered consequential out of pocket losses for procuring credit freeze or

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

171. As a result of Defendant's unlawful business practices, violations of the UCL, Plaintiffs and the Class Members are entitled to injunctive relief.

FIFTH CLAIM
Violation of California's Unfair Competition Law ("UCL")
Unfair Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq*.)
(On behalf of Plaintiffs and the Nationwide Class or, alternatively, the California Subclass)

172. Plaintiffs and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

173. By reason of the conduct alleged herein, Defendant engaged in unfair "business practices" within the meaning of the UCL.

174. Defendant stored Plaintiffs' and Class Members' Private Information in its electronic and consumer information databases. Defendant represented to Plaintiffs and Class Members that their Private Information was secure and that Plaintiffs' and the Class Members' Private Information would remain private. Defendant engaged in unfair acts and business practices by representing that it had secure computer systems when it did not.

175. Even without these misrepresentations, Plaintiffs and the Class Members were entitled to, and did, assume Defendant would take appropriate measures to keep their Private Information safe. Defendant did not disclose at any

time that Plaintiffs' and Class Members' Private Information was vulnerable to hackers because Defendant's data security measures were inadequate and outdated, and Defendant was the only entity in possession of that material information, which it had a duty to disclose.

176. Defendant knew or should have known it did not employ reasonable measures that would have kept Plaintiffs' and the Class Members' Private Information secure and prevented the loss or misuse of Plaintiffs' and the Class Members' Private Information.

177. Defendant violated the UCL by misrepresenting, both by affirmative conduct and by omission, the security of its systems and services, and its ability to safely store Plaintiffs' and the Class Members' Private Information. Defendant also violated the UCL by failing to implement and maintain reasonable security procedures and practices appropriate to protect Private Information, and by failing to immediately notify Plaintiffs and the Class Members of the Data Breach.

178. Defendant also violated its commitment to maintain the confidentiality and security of Plaintiffs' and the Class Members' Private Information, and failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security.

179. **Defendant engaged in unfair business practices under the "balancing test."** The harm caused by Defendant's actions and omissions, as

described in detail above, greatly outweigh any perceived utility. Indeed, Defendant's failure to follow basic data security protocols and misrepresentations to Plaintiffs' and Class Members about Defendant's data security cannot be said to have had any utility at all. All of these actions and omissions were clearly injurious to Plaintiffs and the Class Members, directly causing the harms alleged below.

180. **Defendant engaged in unfair business practices under the "tethering test."** Defendant's actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that ... all individuals have a right of privacy in information pertaining to them.... The increasing use of computers ... has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.") Defendant's acts and omissions, and the injuries caused by them, are thus "comparable to or the same as a violation of the law …" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal. 4th 163, 187.

181. **Defendant engaged in unfair business practices under the "FTC test."** The harm caused by Defendant's actions and omissions, as described in detail above, is substantial in that it affects hundreds of thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiffs' and the Class Members' Private Information to third parties without their consent, diminution in value of their Customer Data, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs' and the Class Members' Private Information remains in Defendant's possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant's actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No.

1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) ("failure to establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security. confidentiality, and integrity of personal information collected from or about consumers" violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining "unfair acts or practices" as those that "cause[ ] or[are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.").

182. Plaintiffs and the Class Members suffered injury in fact and lost money or property as the result of Defendant's unfair business practices. In particular, Plaintiffs and the Class Members have suffered from improper or fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result of the Data Breach. In addition, their Private Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value. Plaintiffs and the Class Members have also suffered consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures.

183. As a result of Defendant's unfair business practices, violations of the UCL, Plaintiffs and the Class Members are entitled to injunctive relief.

SIXTH CLAIM
Breach of Express Contract
(On behalf of Plaintiffs and the Nationwide Class)

184. Plaintiffs and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

185. Plaintiffs and Class Members and Defendant entered into written agreements regarding the services that Defendant was to provide to Plaintiffs and Class members. In response, Plaintiffs and Class Members paid Defendant monies and provided Defendant with their PII as consideration for these agreements. Defendant's privacy page is evidence of Defendant's promise to protect PII.

186. Plaintiffs and Class Members complied with the express contract when they paid Defendant and provided their PII to Defendant.

187. Defendant breached its obligations under the contracts between itself and Plaintiffs and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII.

188. Defendant's breach of express contracts between itself, on the one hand, and Plaintiffs and Class members, on the other hand directly caused the Data Breach.

189. Plaintiffs and all other Class members were damaged by Defendant's breach of express contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk

of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they endure and will continue to endure.

SIXTH CLAIM
Breach of Implied Contract
(On behalf of Plaintiffs and the Nationwide Class)

190. Plaintiffs and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

191. In connection with receiving services from Defendant Plaintiffs and all other Class Members entered into implied contracts with Defendant.

192. Pursuant to these implied contracts, Plaintiffs and Class Members provided Defendant with their PII in order for Defendant to service their loans, for which Defendant is compensated. In exchange, Defendant agreed to, among other things, and Plaintiffs understood that Defendant would: (1) provide services to Plaintiffs and Class Members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs'

and Class members PII in compliance with federal and state laws and regulations and industry standards.

193. Had Plaintiffs and Class Members known that Defendant would not adequately protect its customers' and former customers' PII, they would not have provided Flagstar with their PII.

194. Plaintiffs and Class members performed their obligations under the implied contracts when they provided Flagstar with their PII.

195. Defendant breached its obligations under their implied contracts with Plaintiffs and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiffs' and Class Members' PII in a manner that complies with applicable laws, regulations, and industry standards.

196. Defendant's breach of its obligations of its implied contracts with Plaintiffs and Class Members directly resulted in the Data Breach and the injuries that Plaintiffs and all other Class members have suffered from the Data Breach.

197. Plaintiffs and all other Class Members were damaged by Defendant's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services

for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they endure and will continue to endure.

EIGHTH CLAIM
Declaratory Judgment
(On behalf of Plaintiffs and the Nationwide Class)

198. Plaintiffs and the Class repeat and reallege each and every allegation in the Complaint as if fully set forth herein.

199. Defendant owes duties of care to Plaintiffs and Class Members that require Defendant to adequately secure their PII.

200. Defendant still possess Plaintiffs' and Class Members' PII.

201. Defendant do not specify in the Notice of Data Breach letters what steps they have taken to prevent a data breach from occurring again.

202. Plaintiffs and Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

203. Plaintiffs, therefore, seek a declaration that (1) Defendant's existing security measures do not comply with its duties of care to provide reasonable

security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

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

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendant and that the Court grant the following:

1. An order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

2. An order enjoining Defendant from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiffs and Class Members;

3. An order requiring Defendant to:

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

   b. Engage third-party security auditors and internal personnel to run automated security monitoring;

   c. Audit, test, and train their security personnel regarding any new or modified procedures;

   d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

   e. Conduct regular database scanning and security checks;

   f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

   g. Purchase credit monitoring services for Plaintiffs and Class Members for a period of ten years; and

   h. Meaningfully educate Plaintiffs and Class Members about the threats they face as a result of the loss of their

PII to third parties, as well as the steps they must take to protect themselves.

4. An order instructing Defendant to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;

5. An award of compensatory, statutory, and nominal damages in an amount to be determined at trial;

6. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

7. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demands this matter be tried before a jury.

Respectfully Submitted,

DATE: JUNE 24, 2022

/s/ Bryan L. Bleichner

CHESTNUT CAMBRONNE PA
Bryan L. Bleichner (CAL BAR # 220340)*
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Email: *bbleichner@chesnutcambronne.com*

THE LYON LAW FIRM, LLC
Joseph M. Lyon (OH BAR #76050)*
2754 Erie Ave.
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 766-9011
Email: *jlyon@thelyonfirm.com*

*Admitted in this Court