UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

MICHAEL PERKAJ, individually, and on behalf of all others similarly situated, Plaintiff, v. FLAGSTAR BANCORP, INC. and FLAGSTAR BANK, FSB, Defendants.	Case No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Michael Perkaj ("Plaintiff"), individually, and on behalf of all others similarly situated, by and through his attorneys, brings this action against Flagstar Bancorp, Inc. and Flagstar Bank, FSB (collectively, "Flagstar" or "Defendants"), and alleges, based upon personal knowledge as to his own actions and his counsels' investigation, and based upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Flagstar is a full-service, Michigan-based bank and mortgage lender operating 150 branches across the United States and holding over $23 billion in assets.[1]

2. As a bank and mortgage originator company providing financial services, Flagstar collects, maintains, and stores its clients' highly sensitive personal and financial information including, but not limited to: full names, Social Security numbers, dates of birth, financial account information, payment card numbers, and account access information ("personally identifying information" or "PII").[2]

3. Although Flagstar is a sophisticated entity that provides banking, mortgage, and financial services to clients, Flagstar failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive personal and financial information of approximately 1.5 million individuals, including the Plaintiff and the Class. As a direct, proximate, and foreseeable result of Flagstar's failure to implement reasonable security protections sufficient to prevent an

[1] *About Flagstar*, Flagstar Bank, https://www.flagstar.com/about-flagstar.html (last accessed July 11, 2022) **(Exhibit B)**.

[2] *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml (last accessed July 11, 2022) **(Exhibit C)**.

eminently avoidable cyberattack, unauthorized actors compromised Flagstar's network and accessed millions of client files containing highly-sensitive PII.[3]

4. Specifically, on December 3, 2021, and December 4, 2021 Flagstar's clients' sensitive personal data was compromised when unauthorized actors were able to breach Flagstar's network and access files containing approximately 1,547,169 individual's PII (the "Data Breach").[4]

5. Despite the fact that many of the categories of PII exposed in the Data Breach, such as Social Security numbers, cannot be changed, Flagstar failed to provide notice of the Breach to Plaintiff and other individuals affected by the Data Breach ("the Class") until on or around June 17, 2022—more than two weeks after Flagstar claims to have realized that the Data Breach occurred, and more than **six months** after unauthorized individuals accessed Plaintiff's and Class members' highly sensitive PII stored on Flagstar's systems.

6. On information and belief, Flagstar believed that it had suffered a Data Breach involving its current and former customer's PII prior to June 2, 2022.

7. Flagstar's failure to promptly notify Plaintiff and Class members that their PII was exfiltrated due to Flagstar's security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize,

[3] *Id.*
[4] *Id.*

misuse and/or disseminate that PII before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and the Class will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

8. Flagstar failed to take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to current and former clients the material fact that it lacked appropriate data systems and security practices to secure PII and financial information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to Flagstar's failures, Plaintiff and approximately 1.5 million individuals nationwide suffered substantial harm and injury.

9. As a result of Flagstar's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third-parties for the express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Flagstar's current and former clients. Plaintiff and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors.

10. Plaintiff and Class members suffered injuries as a result of Flagstar's conduct including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized the use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized debits; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise to their PII, which remains in Flagstar's possession and is subject to further unauthorized disclosures so long as Flagstar fails to undertake appropriate and adequate measures to protect their PII. These risks will remain for the lifetimes of Plaintiff and the Class.

11. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief from Flagstar's failure to reasonably safeguard Plaintiff's and Class members' PII; its failure to reasonably provide timely notification that Plaintiff's and Class members' PII had been compromised by an unauthorized third

party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their PII.

II. PARTIES

Plaintiff Michael Perkaj

12. Plaintiff Michael Perkaj ("Plaintiff") is a resident and citizen of Michigan, residing in Brighton, Michigan.

13. Plaintiff received Flagstar's *Notice of Data Breach* (the "Notice"), a copy of which is attached hereto as **Exhibit A**, after June 17, 2022.

14. Plaintiff is a former client of Flagstar. According to the Notice Plaintiff received, Flagstar possessed Plaintiff's PII, including his name, Social Security number, and telephone number, and stored the PII in a file on Flagstar's network.

15. Plaintiff previously maintained a checking account at Flagstar. Plaintiff does not recall exactly when he opened that account, but, to the best of his recollection, believes he opened it in or around 2010, at which time he provided Flagstar with various categories of PII, including but not limited to his name, phone number, and Social Security number. Plaintiff closed that account approximately 10 years ago and, since that time, has not maintained an account, or any other business relationship, with Flagstar.

16. Plaintiff provided his PII to Flagstar with the expectation that Flagstar and its agents would exercise reasonable care to protect and maintain the

confidentiality of his PII and other confidential information by safeguarding it from compromise, disclosure, and misuse by unauthorized actors, except to the extent necessary to provide agreed-upon financial services, and would be timely and forthright relating to any data security incidents involving his PII.

17. In the Notice that Plaintiff received after June 17, 2022, Flagstar informed him that his Social Security number, name, and phone number "were accessed and/or acquired from our network. . . ." Exhibit A. Further, although Flagstar asserted in the Notice that it has "no evidence that any of the information had been misused" Flagstar concedes his PII was exfiltrated. *See* Ex. A at 1 ("certain impacted files containing your personal information were accessed and/or acquired . . .").

18. In acknowledgement of the risks that the Data Breach impose on Plaintiff, Flagstar offered Plaintiff identity monitoring services at no cost for two years, and advised Plaintiff that he should obtain a credit report and place a fraud alert or security freeze on his credit files in order to guard against the concrete risks the Data Breach imposed upon him.

19. The Data Breach already has required Plaintiff to expend significant time and effort to protect himself from its potential adverse consequences, including but not limited to investigating whether hackers have further attempted to misuse his PII, and potential means by which to protect himself from identity theft, such as by

placing fraud alerts on his credit accounts at major credit bureaus, reviewing his credit reports, and monitoring associated bank and credit accounts.

20. Because Plaintiff perpetually will be at risk of identity theft due to the nature of the PII Flagstar failed to safeguard, Plaintiff ultimately elected to purchase at an initial annual cost of $87.99 the ReliaShield product, a suite of tools designed to, *inter alia*, protect Plaintiff from identity theft.

21. As a direct, proximate and foreseeable result of the Data Breach, as well as Flagstar's failure to prevent against and timely notify Plaintiff of the same, Plaintiff has suffered concrete injuries and damages, including out-of-pocket costs incurred in mitigating the immediate effects of the Data Breach and the heightened risk of fraud and identity theft to which the Breach exposed him.

Defendant Flagstar Bank, FSB

22. Defendant Flagstar Bank, FSB is a federally chartered bank organized under the laws of the State of Michigan, with its principal place of business at 5151 Corporate Drive, Troy, Michigan 48098.

Defendant Flagstar Bancorp, Inc.

23. Defendant Flagstar Bancorp, Inc. is a corporation organized under the laws of the State of Michigan, with its principal place of business at 5151 Corporate Drive, Troy, Michigan 48098. Flagstar Bank, FSB is a wholly-owned subsidiary of Flagstar Bancorp, Inc.

III. JURISDICTION AND VENUE

24. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and at least one Class member is a citizen of a state different from Defendants.

25. This Court has personal jurisdiction over Defendants because Defendants are authorized to and regularly conduct business in Michigan, and are headquartered in Troy, Michigan.

26. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Flagstar Bank, FSB - Background

27. Flagstar provides banking, mortgage, and financial services to clients at 150 branches, making Flagstar the sixth largest bank mortgage originator in the country, handling $300 billion in home loans.[5] Flagstar represents to its clients that "protecting [their] finances is a top priority" and that "[t]he only employees who see

[5] *See About Flagstar*, *supra*, footnote 1, Ex. B.

[their] information are those whose job functions require them to review sensitive data."[6]

28. As part of their business operations, Flagstar collects, maintains, and stores the highly sensitive PII and financial information provided by its current and former clients, including but not limited to: full names, Social Security numbers, dates of birth, financial account numbers, payment card information, phone numbers, and account access information.

29. On information and belief, at the time of the Data Breach, and despite its claims that Flagstar has "firewalls and prevention systems that stop unauthorized access to our network and computers, plus secure network protocols that ensure secure connections between our offices, partners, and customers,"[7] Flagstar failed to implement necessary data security safeguards, which resulted in unauthorized third parties accessing the PII of over 1.5 million current and former clients.

30. Current and former clients of Flagstar, such as Plaintiff and the Class, made their PII available to Flagstar with the reasonable expectation that Flagstar would comply with its obligation and promises to keep their sensitive and personal information, including their PII, confidential and secure from illegal and

[6] *Preventing Fraud*, Flagstar Bank, https://www.flagstar.com/fraud-information-center/preventing-fraud.html (last accessed July 11, 2022) **(Exhibit D)**.
[7] *Id.*

unauthorized access, and that Flagstar would provide them with prompt and accurate notice of any unauthorized access to their PII.

31. Unfortunately for Plaintiff and Class members, Flagstar failed to carry out its duty to safeguard this highly sensitive PII and provide adequate data security, thus failing to protect Plaintiff and Class members from the exfiltration of their PII during the Data Breach.

B. The Data Breach

32. Flagstar disclosed in a Notice sent on or about June 17, 2022, to Plaintiff and other affected individuals that it was affected by a "cyber incident that involved unauthorized access to [their] network"—the Data Breach—and that Plaintiff's and other individual's sensitive PII had been compromised. Further, Flagstar acknowledges that the unauthorized actors were able to exfiltrate Plaintiff's and Class members' PII and Social Security numbers, stating that "files containing your personal information were accessed and/or acquired from our network . . ." *See* Exhibit A.

33. According to the Notice, this unauthorized access to Flagstar's network occurred "between December 3, 2021 and December 4, 2021." *See* Exhibit A.

34. Flagstar asserts in the Notice that it did not detect the Data Breach until on or about June 2, 2022, almost ***six months*** after the unauthorized individuals first gained unfettered access to Flagstar's data systems. *See* Exhibit A.

35. Flagstar asserts that upon discovering the Data Breach, at some undisclosed date prior to June 2, 2022, it "activated [its] incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement" that unauthorized actors accessed files containing Flagstar's current and former clients' "Social Security number, name, and phone number." *See* Exhibit A.

36. According to Flagstar, it finally determined on June 2, 2022, that certain files accessed and exfiltrated by the unauthorized individuals in the Data Breach contained personal information of both current and former customers.

37. Despite acquiring knowledge of the unauthorized access on June 2, 2022, Flagstar delayed in sending individualized notice to affected clients until on or after June 17, 2022. *See* Exhibit A.

38. Flagstar has not yet acknowledged the full extent of PII that was improperly accessed by unauthorized third parties in the Data Breach. Flagstar admitted in a filing with the Maine Attorney General that the unauthorized actors gained access to Flagstar's current and former clients' "[n]ame or other personal identifier in combination with: Social Security Number" but failed to specify which types of personal identifiers were accessed.[8]

[8] *See Data Breach Notifications*, *supra*, footnote 2, Ex. C.

39. During the time that the unauthorized individuals had unrestricted access to Flagstar's network, they were able to access and acquire personal, sensitive, and protected PII belonging to over 1.5 million current and former Flagstar clients.

C. Flagstar's Many Failures Both Prior to and Following the Breach

40. Flagstar could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and network files containing PII.

41. In the Notice, Flagstar acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to virtually every aspect of Flagstar's operations as a banking institute. Flagstar acknowledges this fact on their own website, stating "[s]ecuring your financial information is essential to protecting your finances" and that "[p]rotecting your finances is a top priority."[9]

42. Despite such representations, and its purported expertise with "firewalls and prevention systems that stop unauthorized access," Flagstar failed to detect that its own data system was compromised until June 2, 2022.[10]

43. Further, despite detecting the Data Breach on June 2, 2022, Flagstar waited until on or about June 17, 2022, to begin notifying its current and former

[9] *See Preventing Fraud*, supra, footnote 6, Ex. D.
[10] *Id.*

clients of the Data Breach—over six months after the Data Breach occurred, a significant amount of time after it first detected the Data Breach, and more than two weeks after it determined that the unauthorized actors obtained and exfiltrated current and former customers' PII.

44. Moreover, when Flagstar finally acknowledged that it had experienced a breach, it failed to fully inform affected individuals of the length of time that the unauthorized actors had access to their PII, or even the full extent of the PII that was accessed during the Data Breach.

45. Flagstar's failure to properly safeguard Plaintiff's and Class members' PII allowed the unauthorized actors to access this highly sensitive PII and financial information, and Flagstar's failure to timely notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities prior to the dissemination of their PII.

46. The Data Breach also highlights the inadequacies inherent in Flagstar's network monitoring procedures. If Flagstar had properly monitored its cyber security systems, it would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from exfiltrating PII and financial information. The foregoing is particularly true of former Flagstar customers like Plaintiff, many of whom likely did not know that Flagstar continued to maintain their PII on its system, and thus had no reason to think their PII may have been

compromised in the Data Breach. Flagstar's egregious failure to secure PII it had no reason to continue to maintain has now needlessly exposed Plaintiff and other former account holders to a concrete risk of future harm.

47. Flagstar's delayed response only further exacerbated the consequences of the Data Breach brought on by its systemic IT failures.

48. First, Flagstar failed to timely notify affected individuals, including Plaintiff and Class members, that Flagstar had allowed their highly-sensitive PII to be accessed by unauthorized third parties.

49. Second, Flagstar has made no effort to protect Plaintiff and the Class from the long-term consequences of Flagstar's acts and omissions. Although the Notice offered victims a complimentary two year membership to Kroll's credit monitoring services, Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long beyond two years. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives, a risk that only two years of credit monitoring cannot remedy.

50. In short, Flagstar's myriad failures, including to timely detect the Data Breach and to notify Plaintiff and Class members with reasonable timeliness that their personal and financial information had been exfiltrated due to Flagstar's security failures, allowed unauthorized individuals to access and misappropriate

Plaintiff's and Class members' PII for months before Flagstar finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

51. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, including Social Security numbers and financial account information in particular, is an invaluable commodity and a frequent target of hackers. Flagstar acknowledges this fact on its own website, stating "[r]apid advances in technology and creative criminal minds make fraud a potentially serious threat on a variety of fronts."[11]

52. In 2019, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[12]

53. Of the 1,473 recorded data breaches, 108 of them were in the banking/credit/financial industry, with the number of sensitive records being

[11] *See Preventing Fraud*, *supra*, footnote 6, Ex. D.
[12] *2019 End of Year Data Breach Report*, Identity Theft Resource Center (Jan. 8, 2020), available at: https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed July 11, 2022) **(Exhibit E)**.

exposed exceeding 100 million. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in those 108 breaches in the banking/credit/financial sector.[13]

54. The 108 reported financial sector data breaches reported in 2019 exposed 100,621,770 sensitive records, compared to 2018 in which only 1,778,658 sensitive records were exposed in financial sector breaches.[14]

55. In fact, Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach incidents.[15] Conditions have only worsened since: Statista estimates that "[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]" and that "[i]n the first half of 2020, there were 540 reported data breaches."[16]

---

[13] *Id.*
[14] *Id.*
[15] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista (Aug. 2020), available at: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed (last accessed July 11, 2022) **(Exhibit F)**.
[16] *Id.*

56. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

57. Individuals are particularly concerned with protecting the privacy of their financial account information and Social Security numbers. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start."

58. In light of recent high profile data breaches at other industry leading companies, including, Equifax (147 million records, September 2017), Heartland Bank (130 million records, January 2008), Capital One Bank (100 million records, March 2019), JPMorgan Chase (83 million records, October 2014), Experian (24 million records, August 2020), First American Financial (885 million records, May 2019), Microsoft (250 million records, December 2019), Wattpad (268 million

records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), and Whisper (900 million records, March 2020), Flagstar knew or should have known that its electronic records would be targeted by cybercriminals.

59. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

60. Protecting banking customers' PII is of such vital importance that Congress enacted the Gramm–Leach–Bliley Act, which, *inter alia*, imposes "an affirmative and continuing obligation" on all financial institutions to "respect the privacy of [their] customers and to protect the security and confidentiality of those customers' nonpublic personal information." 15 U.S.C. § 6801. In furtherance of that duty, institutions are required to establish appropriate safeguards "to insure the security and confidentiality of customer records and information; to protect against any anticipated threats or hazards to the security or integrity of such records; and to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer." *Id.*

61. Consumers' PII 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.

62. Compromised Social Security numbers pose the greatest risk to consumers 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 happened here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[17]

63. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. 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.

[17] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed July 11, 2022) **(Exhibit G)**.

64. 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 information and Social Security Numbers are worth more than 10x on the black market."[18]

65. Given the nature of Flagstar's Data Breach, as well as the length of the time Flagstar's networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' PII can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in Class members' names.

66. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

---

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), available at http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed July 11, 2022) **(Exhibit H)**.

67. To date, Flagstar has offered its consumers *only two years* of identity monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the threats they face for years to come, particularly in light of the PII at issue here.

68. Despite the prevalence of public announcements of data breaches and data security compromises, its own expertise in the information technology sector, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep PII private and secure, Flagstar failed to take appropriate steps to protect the PII of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Flagstar's failure to implement or maintain adequate data security measures for its current and former clients.

E. Flagstar Had a Duty and Obligation to Protect PII

69. Flagstar has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII. Flagstar's obligations are derived from: 1) government regulations and state laws, and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided, and Flagstar obtained, their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

70. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[19] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[20]

71. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.

72. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[21] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

[19] 17 C.F.R. § 248.201 (2013).
[20] *Id.*
[21] *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n (Oct. 2016), available at: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed July 11, 2022) **(Exhibit I)**.

networks; understand their network's vulnerabilities; and implement policies to correct security problems.[22] 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.[23] Flagstar clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, and the amount of data exfiltrated.

73. Here, at all relevant times, Flagstar was fully aware of its obligation to protect the PII of its current and former clients, including Plaintiff and the Class, representing to its customers that "[s]ecuring [clients'] financial information is essential to protecting [clients'] finances" and Flagstar is a sophisticated and technologically savvy financial and banking institution that relies extensively on technology systems and networks, and routinely maintains and transmits clients' PII and financial information in order to operate its business.[24]

74. Flagstar had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the PII and financial information of its current and former customers from the foreseeable risk of a data breach. The duty arises out of

[22] *Id.*
[23] *Id.*
[24] *See Preventing Fraud*, *supra*, footnote 6, Ex. D.

the special relationship that exists between Flagstar and Plaintiff and Class members. Flagstar alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' PII.

75. Flagstar's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential client data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

76. Further, Flagstar had a duty to promptly notify Plaintiff and the Class that their PII was accessed by unauthorized persons.

F. Flagstar Violated FTC and Industry Standard Data Protection Protocols

77. The FTC rules, regulations, and guidelines obligate businesses to protect PII, from unauthorized access or disclosure by unauthorized persons.

78. Unfortunately, Flagstar failed to comply with FTC rules, regulations and guidelines, and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Flagstar failed in, *inter alia*, the following respects:

a. Developing and employing adequate intrusion detection systems;

b. Engaging in regular reviews of audit logs and authentication records;

c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

d. Ensuring the confidentiality and integrity of current and former clients' PII;

e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its current and former clients' PII;

f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

h. Implementing technical policies, procedures and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

i. Other similar measures to protect the security and confidentiality of its current and former clients' PII.

79. Had Flagstar implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Flagstar could have prevented or detected the Data Breach prior to the unauthorized actors accessing Flagstar's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former clients of Flagstar would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. Flagstar's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

80. Flagstar purports to care about data security and safeguarding clients' PII, and represents that it will keep secure and confidential the PII belonging to its current and former clients.

81. Plaintiff's and Class members' PII and financial information was provided to Flagstar in reliance on its promises and self-imposed obligations to keep PII and financial information confidential, and to secure the PII and financial information from unauthorized access by malevolent actors. It failed to do so.

82. The length of the Data Breach also demonstrates that Flagstar failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors periodically to test its network, servers, systems and workstations.

83. Had Flagstar undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Flagstar would have detected the Data Breach prior to the hackers extracting data from Flagstar's networks, and Flagstar's current and former customers would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

84. Indeed, following the Data Breach, Flagstar effectively conceded that its security practices were inadequate and ineffective. In the Notice it sent to Plaintiff and others, Flagstar acknowledged that the Data Breach required it to implement multiple remedial measures to protect its current and former clients from the unauthorized access of "files containing [their] personal information were accessed and/or acquired from [its] network. . . ." *See* Exhibit A.

H. Plaintiff and the Class Suffered Harm Resulting from the Data Breach

85. Like any data hack, the Data Breach presents major problems for all affected. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance."[25]

86. The ramifications of Flagstar's failure to properly secure PII, including Plaintiff's and Class members' PII, are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission to commit fraud or other crimes.

[25] *Warning Signs of Identity Theft*, Federal Trade Comm'n, available at: https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft (last accessed July 11, 2022) **(Exhibit J)**.

87. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

88. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

89. Accordingly, Flagstar's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[26] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Plaintiff's and Class members' PII will do so at a later date or re-sell it.

90. In response to the Data Breach, Flagstar offered to provide certain individuals whose PII was exposed in the Data Breach with two years of credit monitoring. However, two years of complimentary credit monitoring is a time period

[26] Al Pascual, *The Consumer Data Insecurity Report: Examining the Data Breach-Identity Fraud Paradigm in Four Major Metropolitan Areas*, National Consumer League (June 2014), available at: https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf (last accessed July 11, 2022) **(Exhibit K)**.

much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by Flagstar's failures.

91. Moreover, the credit monitoring offered by Flagstar is inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive PII.

92. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Flagstar's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

93. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being accessed by cybercriminals, risks that will not abate within a mere two years: the unauthorized access of Plaintiff's and Class members' PII, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Flagstar offered victims of the Breach. The two years of credit monitoring that Flagstar offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class members have suffered and will continue to suffer as a result of the Data Breach.

94. As a direct and proximate result of Flagstar's acts and omissions in failing to protect and secure PII and financial information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

95. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach

on behalf of both himself and similarly situated individuals whose PII was accessed in the Data Breach.

96. Flagstar is aware of the ongoing harm that the Data Breach has and will continue to impose on Flagstar's current and former clients, as the notices that it posted and sent to Plaintiff and Class members regarding the Data Breach advise the victims to place "a fraud alert and/or security freeze on [their] credit files, and/or obtain[] a free credit report." *See* Exhibit A.

V. CLASS ALLEGATIONS

97. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All persons in the United States whose PII was accessed in the Data Breach.

Excluded from the Class are Defendants, their executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

98. In the alternative, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All persons who are residents of the State of Michigan whose PII was accessed in the Data Breach (the "Michigan Subclass").

Excluded from the Michigan Subclass are Defendants, their executives and officers, and the Judge(s) assigned to this case.

99. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Flagstar and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that more than 1.5 million individuals comprise the Class and were affected by the Data Breach. Indeed, Flagstar admitted that the Data Breach affected more than 1.5 million individuals in its notification to the Maine Attorney General's Office.[27] The members of the Class will be identifiable through information and records in Flagstar's possession, custody, and control.

100. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Flagstar's data security and retention policies were unreasonable;

b. Whether Flagstar failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Flagstar owed a duty to Plaintiff and Class members to safeguard their PII;

[27] *See Data Breach Notifications*, *supra*, footnote 2, Ex. C.

d. Whether Flagstar breached any legal duties in connection with the Data Breach;

e. Whether Flagstar's conduct was intentional, reckless, willful or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether Flagstar breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Flagstar's conduct; and

i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

101. Typicality: All of Plaintiff's claims are typical of the claims of the Class as Plaintiff and all members of the Class had their PII compromised in the Data Breach. Plaintiff and the members of the Class sustained damages as a result of Flagstar's uniform wrongful conduct.

102. Adequacy: Plaintiff is an adequate representative because his interests do not materially or irreconcilably conflict with the interests of the Class he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither

Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

103. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Flagstar's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Flagstar's records and databases.

104. Flagstar has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

VI. CAUSES OF ACTION

COUNT I — Negligence
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

105. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

106. This count is brought on behalf of all Class members.

107. Flagstar owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Flagstar collected.

108. Flagstar owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Flagstar collected.

109. Flagstar owed a duty to Plaintiff and the Class to implement processes to detect a data breach quickly, to act timely on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

110. Flagstar owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

111. Flagstar solicited, gathered, and stored the PII belonging to Plaintiff and the Class.

112. Flagstar knew or should have known it inadequately safeguarded this information.

113. Flagstar knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and the Class, and therefore Flagstar was charged with a duty to provide adequate protections for this critically sensitive information.

114. Flagstar had a special relationship with Plaintiff and the Class. Plaintiff's and Class members' highly sensitive PII and financial information was entrusted to Flagstar on the understanding that adequate security precautions would be taken to protect the PII and financial information. Moreover, only Flagstar had the ability to protect its systems and the PII stored on them from attack.

115. Flagstar's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. Flagstar's misconduct included failing to: (1) secure its systems, servers and networks, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

116. Flagstar breached its duties to Plaintiff and the Class by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiff and the Class.

117. Flagstar breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

118. Flagstar breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

119. The law further imposes an affirmative duty on Flagstar to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

120. Flagstar failed to return, purge, or delete the PII belonging to Plaintiff and other former customers of Flagstar at the conclusion of their banking relationship and within the time limits allowed by law.

121. Flagstar breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their PII had been improperly acquired or accessed.

122. Flagstar breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about June 17, 2022.

123. As a direct and proximate result of Flagstar's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

124. As a direct and proximate result of Flagstar's conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II — Negligence *Per Se*
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

125. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Flagstar, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Flagstar's duty.

126. The Michigan Identity Theft Protection Act ("MITPA) requires that entities in possession of PII belonging to Michigan residents that was or may have been accessed by unauthorized persons disclose the data breach without unreasonable delay. *See* Mich. Comp. Laws § 445.72(4).

127. The Michigan Consumer Protection Act ("MCPA") requires that entities in possession of PII belonging to Michigan residents to: 1) protect PII from

unauthorized access and disclosure, and 2) maintain reasonable security practices. *See* Mich. Comp. Laws § 445.903(1).

128. In addition to the FTC rules and regulations, the MITPA, and MCPA, other states and jurisdictions where victims of the Data Breach are located require that Flagstar protect PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

129. Flagstar violated the MITPA, the MCPA and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Flagstar's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiff's and Class members' sensitive PII.

130. Flagstar's violations of the MITPA, the MCPA, the FTC Act and other applicable statutes, rules, and regulations constitutes negligence *per se*.

131. Plaintiff and the Class are within the category of persons the MITPA, the MCPA and the FTC Act were intended to protect.

132. The harm that occurred as a result of the Data Breach described herein is the type of harm the MITPA, the MCPA and FTC Act were intended to guard against.

133. As a direct and proximate result of Flagstar's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Flagstar's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III — Breach of Implied Contract
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

135. This count is brought on behalf of all Class members.

136. Plaintiff and the Class provided Flagstar with their PII and financial information.

137. By providing their PII, and upon Flagstar's acceptance of such information, Plaintiff and the Class, on one hand, and Flagstar, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

138. The implied contracts between Flagstar and Plaintiff and Class members obligated Flagstar to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged

above. Flagstar expressly adopted and assented to these terms in its public statements, representations and promises as described above.

139. The implied contracts for data security also obligated Flagstar to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII.

140. Flagstar breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' PII; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

141. As a direct and proximate result of Flagstar's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII in Flagstar's possession, and are entitled to damages in an amount to be proven at trial.

COUNT IV — Bailment
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

142. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

143. This count is brought on behalf of all Class members.

144. Plaintiff and Class members provide their PII to Flagstar.

145. In delivering their PII, Plaintiff and Class members intended and understood that their PII would be safeguarded and protected.

146. Flagstar accepted Plaintiff's and Class members' PII.

147. By accepting possession of Plaintiff's and Class members' PII, Flagstar understood that Plaintiff and the Class expected their PII to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

148. During the bailment (or deposit), Flagstar owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their PII.

149. Flagstar breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII.

150. Flagstar further breached its duty to safeguard Plaintiff's and Class members' PII by failing to timely notify them that their PII had been compromised as a result of the Data Breach.

151. Flagstar failed to return, purge, or delete the PII belonging to Plaintiff and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

152. As a direct and proximate result of Flagstar's breach of its duties, Plaintiff and the Class suffered consequential damages that were reasonably foreseeable to Flagstar, including but not limited to the damages set forth herein.

153. As a direct and proximate result of Flagstar's breach of its duty, Plaintiff's and Class members PII that was entrusted to Flagstar during the bailment (or deposit) was damaged and its value diminished.

COUNT V — Violation of the Michigan Consumer Protection Act
Mich. Comp. Laws Ann. § 445.903, *et seq.*
(On behalf of the Class, or, in the alternative the Michigan Subclass)

154. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

155. This count is brought on behalf of the Michigan Subclass.

156. The Michigan Consumer Protection Act ("MCPA"), Mich. Comp. Laws § 445.903, *et seq.*, prohibits "[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce . . . ." Mich. Comp. Laws § 445.903(1).

157. Flagstar engaged in deceptive trade practices in the course of its business, in violation of MCPA, Section 445.903(1), including:

a. Representing that services have characteristics or benefits that they do not have;

b. Representing that services are of a particular standard or quality if they are of another;

c. Advertising services with the intent not to dispose of the services as advertised;

d. Advertising services with intent not to supply reasonably expectable public demand;

e. Failing to reveal a material fact which tends to mislead or deceive the consumer;

f. Making a representation of fact material to the transaction so that a person reasonably believes the represented state of affairs to be other than it actually is;

g. Failing to reveal facts material to the transaction in light of representations made in a positive manner.

158. Flagstar's deceptive acts, omissions, and conduct include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

159. Flagstar had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' PII. This exclusive knowledge includes, but is not limited to, information that Flagstar received through internal and other non-public audits and reviews that concluded that Flagstar's security policies were substandard and deficient, and that Plaintiff's and Class members' PII and other Flagstar data was vulnerable.

160. Flagstar had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

161. Flagstar also had exclusive knowledge about the length of time that it maintained individual's PII after they stopped using Flagstar's services.

162. Flagstar failed to disclose, and actively concealed, the material information it had regarding Flagstar's deficient security policies and practices, and regarding the security of the sensitive PII and financial information. For example, even though Flagstar has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' PII was vulnerable as a result, Flagstar failed to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. Flagstar also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former clients' PII and other records. Likewise, during the days and weeks following the Data Breach, Flagstar failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

163. Flagstar had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Flagstar was in a fiduciary position by virtue of the fact that Flagstar collected and maintained Plaintiff's and Class members' PII and financial information.

164. Flagstar's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Flagstar's data

security and its ability to protect the confidentiality of current and former clients' PII.

165. Had Flagstar disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Flagstar would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Flagstar received, maintained, and compiled Plaintiff's and Class members' PII without advising that Flagstar's data security practices were insufficient to maintain the safety and confidentiality of their PII.

166. Accordingly, Plaintiff and Class members acted reasonably in relying on Flagstar's misrepresentations and omissions, the truth of which they could not have discovered.

167. Flagstar's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as the MITPA, MCPA and FTC Act.

168. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should have reasonably avoided.

169. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Flagstar's deceptive acts and practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to Flagstar as their clients, and with the understanding that Flagstar would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Flagstar and which is subject to further breaches so long as

Flagstar fails to undertake appropriate and adequate measures to protect data in its possession.

170. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Flagstar from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VI — Violation of State Data Breach Statutes
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

171. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

172. This count is brought on behalf of all Class members.

173. Flagstar is a corporation that owns, maintains, and records PII, and computerized data including PII, about its current and former clients, including Plaintiff and Class members.

174. Flagstar is in possession of PII belonging to Plaintiff and Class members and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

175. Flagstar failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

176. Flagstar, knowing and/or reasonably believing that Plaintiff's and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members as required by following data breach statutes.

177. Flagstar's failure to provide timely and accurate notice of the Data Breach violated the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq.*;

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.80, *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), *et seq.*;

ee. S.C. Code Ann. § 39-1-90(A), *et seq.*;

ff. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), *et seq.*;

hh. Utah Code Ann. § 13-44-202(1), *et seq.*;

ii. Va. Code. Ann. § 18.2-186.6(B), *et seq.*;

jj. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*;

kk. Wis. Stat. Ann. § 134.98(2), *et seq.*; and

ll. Wyo. Stat. Ann. § 40-12-502(a), *et seq.*

178. As a result of Flagstar's failure to reasonably safeguard Plaintiff's and Class members' PII, and the failure to provide reasonable and timely notice of the Data Breach to Plaintiff and Class members, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Flagstar's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VII — Violation of State Consumer Protection Statutes
(On behalf of the Class)

179. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

180. This count is brought on behalf of all Class members.

181. Flagstar is a "person" as defined in the relevant state consumer statutes.

182. Flagstar engaged in the conduct alleged herein that was intended to result, and which did result, in the trade and commerce with Plaintiff and Class members. Flagstar is engaged in, and its acts and omissions affect, trade and commerce. Further, Flagstar's conduct implicates consumer protection concerns generally.

183. Flagstar's acts, practices and omissions were done in the course of Flagstar's business of marketing, facilitating, offering for sale, and selling goods and services throughout the United States.

184. Flagstar's unlawful, unfair, deceptive, fraudulent and/or unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act and similar state laws, rules, and regulations, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties

pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and Class members that their PII was accessed by unauthorized persons in the Data Breach.

185. By engaging in such conduct and omissions of material facts, Flagstar has violated state consumer laws prohibiting representing that "goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have," representing that "goods and services are of a particular standard, quality or grade, if they are of another" and/or "engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding"; and state consumer laws prohibiting unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices.

186. Flagstar's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Flagstar's data security and ability to protect the confidentiality of PII.

187. Flagstar intentionally, knowingly, and maliciously misled Plaintiff and Class members and induced them to rely on its misrepresentations and omissions.

188. Had Flagstar disclosed that its data systems were not secure and, thus, vulnerable to attack, it would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Flagstar received, maintained, and compiled Plaintiff's and Class

members' PII without advising that Flagstar's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and the Class members acted reasonably in relying on Flagstar's misrepresentations and omissions, the truth of which they could not have discovered.

189. Past breaches within the industry put Flagstar on notice that its security and privacy protections were inadequate.

190. Flagstar's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like the MITPA, MCPA, and the FTC Act.

191. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

192. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of Flagstar's unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and/or unlawful acts or practices as set forth herein include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal and financial information entrusted to Flagstar and with the understanding that Flagstar would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Flagstar and which is subject to further breaches so long as Flagstar fails to undertake appropriate and adequate measures to protect data in its possession.

193. Flagstar's conduct described herein, including without limitation, Flagstar's failure to maintain adequate computer systems and data security practices to safeguard Plaintiff's and Class members' PII, Flagstar's failure to disclose the material fact that it did not have adequate computer systems and safeguards to adequately protect Plaintiff's and Class members' PII, Flagstar's failure to provide

timely and accurate notice to of the material fact of the Data Breach, and Flagstar's continued acceptance of Plaintiff's and Class members' PII constitute unfair methods of competition and unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices in violation of the following state consumer statutes:

a. The Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5(5), (7) and (27), *et seq*.;

b. The Arizona Consumer Fraud Act, A.R.S. § 44-1522;

c. The Arkansas Deceptive Trade Practices Act, Ark. Code Ann. §§ 4-88-107(a)(1)(10) and 4-88-108(1)(2), *et seq*.;

d. The California Consumer Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., and the California Unfair Competition Law, Cal. Bus. and Prof. Code, § 17200, *et seq*.;

e. The Connecticut Unfair Trade Practices Act, Conn. Gen. Stat. § 42-110(b), *et seq*.;

f. The Delaware Deceptive Trade Practices Act, Del. Code Ann. Title 6, § 2532(5) and (7), *et seq*., and the Delaware Consumer Fraud Act, Del. Code Ann. Title 6 § 2513, *et seq*.;

g. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq*.;

h. The Georgia Fair Business Practices Act, Ga. Code Ann. §§ 10-1-393(a) and (b)(2), (5) and (7), *et seq*.;

i. The Hawaii Deceptive Trade Practices Act, Haw. Rev. Stat. Ann. §§ 481A-3(a)(5), (7) and (12), *et seq*.; and the Hawaii Consumer Protection Act, Haw. Rev. Stat. Ann. § 480-2(a), *et seq*.;

j. The Idaho Consumer Protection Act, Idaho Code §§ 48-603(5), (7), (17) and (18), *et seq*.; and Idaho Code § 48-603C, *et seq*.;

k. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Stat. § 505/2, *et seq*.;

l. The Indiana Deceptive Consumer Sales Act, Ind. Code §§ 24-5-0.5-3(a) and (b)(1) and (2), *et seq.*;

m. The Iowa Consumer Fraud Act, I.C.A. §§ 714H.3 and 714H.5, *et seq.*;

n. The Kansas Consumer Protection Act, Kan. Stat. §§ 50-626(a) and (b)(1)(A)(D) and (b)(3), *et seq.*;

o. The Kentucky Consumer Protection Act, K.R.S. § 367.170(1) and (2), *et seq.*;

p. The Louisiana Unfair Trade Practices and Consumer Protection Law, La. Rev. Stat. Ann. § 51:1405(A), *et seq.*;

q. The Maine Uniform Deceptive Trade Practices Act, 10 M.R.S.A. §§ 1212(1)(E) and (G), e*t seq.*, and the Maine Unfair Trade Practices Act, 5 M.R.S.A. § 207, *et seq.*;

r. The Maryland Consumer Protection Act, Md. Code Commercial Law, § 13-301(1) and (2)(i), and (iv) and (9)(i), *et seq.*;

s. The Massachusetts Consumer Protection Act, Ma. Gen. Laws Ann. Ch. 93A § 2(a), *et seq.*;

t. The Michigan Consumer Protection Act, M.C.P.L.A. § 445.903(1)(c)(e),(s) and (cc), *et seq.*;

u. The Minnesota Uniform Deceptive Trade Practices Act, Minn. Stat. § 325D.44, subd. 1(5), (7) and (13), et seq., the Minnesota Consumer Fraud Act, Minn. Stat. § 325F.69, subd. 1, and Minn. Stat. § 8.31, subd. 3(a);

v. The Mississippi Consumer Protection Act, Miss. Code Ann. §§ 75-24-5(1), (2)(e) and (g), *et seq.*;

w. The Missouri Merchandising Practices Act, Mo. Ann. Stat. § 407.020(1), *et seq.*;

x. The Montana Unfair Trade Practices and Consumer Protection Act, MCA §§ 30-14-103, *et seq.*;

y. The Nebraska Consumer Protection Act, Neb. Rev. Stat. § 59-1602, and the Nebraska Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-302(a)(5) and (7), *et seq.*;

z. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915(5) and (7), *et seq.*;

aa. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2(v) and (vii), *et seq.*;

bb. The New Jersey Consumer Fraud Act, N.J. Stat. Ann. § 56:8-2, *et seq.*;

cc. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(5)(7) and (14) and 57-12-3, *et seq.*;

dd. New York Business Law, N.Y. Gen. Bus. Law § 349(a);

ee. The North Carolina Unfair Trade Practices Act N.C.G.S.A. § 75-1.1(a), *et seq.*;

ff. The North Dakota Unlawful Sales or Advertising Practices Act, N.D. Cent. Code § 51-15-02, *et seq.*;

gg. The Ohio Consumer Sales Practices Act, Ohio Rev. Code Ann. § 1345.02(A) and (B)(1) and (2), *et seq.*;

hh. The Oklahoma Consumer Protection Act, 15 Okl. Stat. Ann. § 753(5), (7) and (20), *et seq.*; and the Oklahoma Deceptive Trade Practices Act, 78 Okl. Stat. Ann. § 53(A)(5) and (7), *et seq.*;

ii. The Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)(e)(g) and (u), *et seq.*;

jj. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 P.S. §§ 201-2(4)(v)(vii) and (xxi), and 201-3, *et seq.*;

kk. The Rhode Island Deceptive Trade Practices Act, R.I. Gen. Laws § 6-13.1-1(6)(v), (vii), (xii), (xiii) and (xiv), *et seq.*;

ll. The South Carolina Unfair Trade Practices Act, S.C. Code Ann. § 39-5-20(a), *et seq.*;

mm. The South Dakota Deceptive Trade Practices Act and Consumer Protection Act, S.D. Codified Laws § 37-24-6(1), *et seq*.;

nn. The Tennessee Consumer Protection Act, Tenn. Code Ann. §§ 47-18-104(a) and (b)(5) and (7);

oo. The Texas Deceptive Trade Practices- Consumer Protection Act, V.T.C.A., Bus. & C. § 17.46(a), (b)(5) and (7), *et seq*.;

pp. The Utah Consumer Sales Practices Act, Utah Code Ann. §§ 13-11-4(1) and (2)(a) and (b);

qq. The Vermont Consumer Fraud Act, 9 V.S.A. § 2453(a), *et seq.*;

rr. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(5)(6) and (14), *et seq.*;

ss. The Washington Consumer Protection Act, Wash. Rev. Code § 19.86.020, *et seq*.;

tt. The West Virginia Consumer Credit and Protection Act, W.V.A. Code § 46A-6-104, *et seq*.;

uu. The Wisconsin Deceptive Trade Practices Act, W.S.A. § 100.20(1), *et seq.*; and

vv. The Wyoming Consumer Protection Act, Wyo. Stat. Ann. § 40-12-105(a), (i), (iii) and (xv), *et seq*.

194. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Flagstar from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VIII — Unjust Enrichment
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

195. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

196. This count is brought on behalf of all Class members.

197. Plaintiff and the Class have an interest, both equitable and legal, in their PII and financial information that was collected and maintained by Flagstar.

198. Flagstar was benefitted by the conferral upon it of Plaintiff's and Class members' PII and by its ability to retain and use that information. Flagstar understood that it was in fact so benefitted.

199. Flagstar also understood and appreciated that Plaintiff's and Class members' PII and financial information was private and confidential and its value depended upon Flagstar maintaining the privacy and confidentiality of that information.

200. But for Flagstar's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provide or authorized their PII to be provided to Flagstar, and Flagstar would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining clients, gaining the reputational advantages conferred upon it by Plaintiff and Class

members, collecting excessive advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

201. As a result of Flagstar's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that PII) Flagstar has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

202. Flagstar's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

203. Under the common law doctrine of unjust enrichment, it is inequitable for Flagstar to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Flagstar's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

204. The benefit conferred upon, received, and enjoyed by Flagstar was not conferred officiously or gratuitously, and it would be inequitable and unjust for Flagstar to retain the benefit.

205. Flagstar is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Flagstar as a result of its wrongful conduct, including specifically the value to Flagstar of the PII and financial information that was accessed and exfiltrated in the Data Breach and the profits Flagstar receives from the use and sale of that information.

COUNT IX — Declaratory Judgment
(On behalf of the Class, or, in the alternative, the Michigan Subclass)

206. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

207. This count is brought on behalf of all Class members.

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

209. An actual controversy has arisen in the wake of the Data Breach regarding Flagstar's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether Flagstar is

currently maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Flagstar's data security measures remain inadequate.

210. Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

211. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Flagstar continues to owe a legal duty to secure Plaintiff's and Class members' PII, to timely notify them of any data breach, and to establish and implement data security measures that are adequate to secure PII.

212. The Court also should issue corresponding prospective injunctive relief requiring Flagstar to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class members' PII.

213. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy. The threat of another breach of the PII in Flagstar's possession, custody, and control is real, immediate, and substantial. If another breach of Flagstar's network, systems, servers, or workstations occurs, Plaintiff and the Class will not have an adequate remedy at law,

because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

214. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Flagstar if an injunction is issued. Among other things, if another massive data breach occurs at Flagstar, Plaintiff and the Class will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Flagstar of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Flagstar has a pre-existing legal obligation to employ such measures.

215. Issuance of the requested injunction will serve the public interest by preventing another data breach at Flagstar, thus eliminating additional injuries to Plaintiff and the thousands of Class members whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Flagstar, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil

Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Flagstar from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative Class, demand a trial by jury on all issues so triable.

Date: July 11, 2022

Respectfully Submitted,

/s/ Daniel O. Herrera
Daniel O. Herrera (IL BAR #6296731)
Nickolas J. Hagman (IL BAR #6317689)
Olivia Lawless (IL BAR # 6337720)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com
olawless@caffertyclobes.com

Patrick E. Cafferty (MI BAR # 35613)
CAFFERTYCLOBES MERIWETHER & SPRENGEL LLP
220 Collingwood Dr., Suite 130
Ann Arbor, MI 48103
pcafferty@caffertyclobes.com

Attorneys for Plaintiff and the Proposed Class

TABLE OF EXHIBITS

EXHIBIT	DESCRIPTION
Exhibit A	Notice of Data Breach
Exhibit B	*About Flagstar*
Exhibit C	*Data Breach Notifications*
Exhibit D	*Preventing Fraud*
Exhibit E	*End of Year Data Breach Report*
Exhibit F	*Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*
Exhibit G	*Identity Theft and Your Social Security Number*
Exhibit H	*Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*
Exhibit I	*Protecting Personal Information: A Guide for Business*
Exhibit J	*Warning Signs of Identity Theft*
Exhibit K	*The Consumer Data Insecurity Report: Examining the Data Breach- Identity Fraud Paradigm in Four Major Metropolitan Areas*