THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

PHILIP ANGUS and **MARK WIEDDER**, on behalf of themselves and all others similarly situated, Plaintiffs, vs. **FLAGSTAR BANK, FSB**, a Michigan-based federally chartered stock savings bank, Defendant.	Case No.:

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiffs Philip Angus and Mark Wiedder ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Flagstar Bank, FSB ("Defendant"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personally identifiable information that Defendant stored on and/or shared using its vendor's file sharing platform, including, without limitation, names, Social Security numbers, home addresses, phone numbers, dates

of birth, and/or financial account numbers (collectively, "personally identifiable information" or "PII").[1]

2. According to its website, Defendant "has assets of $31.0 billion, is the sixth largest bank mortgage originator nationally, and the second largest savings bank in the country."[2] Defendant "operate[s] 150 branches in Michigan, Indiana, California, Wisconsin, and Ohio and provide[s] a full complement of products and services for consumers and businesses."[3] Its "mortgage division operates nationally through 103 retail locations and a wholesale network of approximately 2,350 third-party mortgage originators."[4]

3. Defendant's customers entrust Defendant with an extensive amount of their PII. Defendant retains this information on computer hardware—even after the customer relationship ends. Defendant asserts that it understands the importance of protecting such information.

---

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number).

[2] *See* https://www.flagstar.com/about-flagstar.html (last visited Mar. 23, 2021).

[3] *Id.*

[4] *Id.*

4. On or before January 22, 2021, Defendant learned that an unauthorized actor breached Defendant's vendor's file sharing platform, which Defendant had used to store and/or share the PII of Plaintiffs and Class Members (the "Data Breach").

5. On or before March 6, 2021, Defendant learned that, during the Data Breach, the unauthorized actor removed one or more documents that contained the PII of Plaintiffs and Class Members, including, but not limited to, names, Social Security numbers, home addresses, phone numbers, dates of birth, and/or financial account numbers.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties to those individuals.

7. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

8. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII of Plaintiffs and Class Members.

9. Plaintiffs bring this action on behalf of all persons whose PII was

compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII of Plaintiffs and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

10. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

11. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized

disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

12. Plaintiff Philip Angus is a citizen of Florida residing in St. Johns County, Florida.

13. Plaintiff Mark Wiedder is a citizen of California residing in Orange County, California.

14. Defendant Flagstar Bank, FSB is a Michigan-based federally chartered stock savings bank, headquartered at 5151 Corporate Drive, Troy, Michigan.

15. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

16. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one other Class Member (including named Plaintiff Philip Angus, a citizen of Florida) is a citizen of a state different from Defendant to establish minimal diversity.

18. The Eastern District of Michigan has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Michigan and this District through its headquarters, offices, parents, and affiliates.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

20. Defendant used its vendor's file sharing platform to store and/or share

some of Plaintiffs' and Class Members most sensitive and confidential information, including names, Social Security numbers, home addresses, phone numbers, dates of birth, financial account numbers, and other personal identifiable information, which is static, does not change, and can be used to commit myriad financial crimes.

21. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

22. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

The Data Breach

23. On or about March 15, 2021, Defendant sent Plaintiff Angus a *Notice of Data Breach*.[5] Defendant informed Plaintiff Angus as follows:

> ***What Happened?***
>
> Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021 that the platform had a vulnerability that was exploited by an unauthorized party. Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access

[5] *See Notice of Data Breach*, a true and correct copy of which is attached hereto as Exhibit 1 ("Ex. 1").

some of Flagstar's information on the Accellion platform – and that we are one of numerous Accellion clients who were impacted.

Flagstar remains fully operational and other parts of our IT infrastructure outside of the Accellion platform were not impacted. Importantly, the Accellion platform was segmented from the rest of our network, and our core banking and mortgage systems were not affected.

What We Are Doing.

Upon learning of the vulnerability, Flagstar promptly took the Accellion server offline and permanently discontinued use of this file sharing platform. Additionally, we acted immediately to contain the threat and engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. As part of our investigation, we have also notified law enforcement.

What Information Was Involved?

On March 6, 2021, we determined that one or more of the documents removed from the Accellion platform contained your Social Security Number, First Name, Last Name, Phone Number, Address.

What You Can Do.

Out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional

> information describing your services is included with this letter.[6]

24. On or about March 12, 2021, Defendant notified various state Attorneys General of the Data Breach. Defendant also provided the Attorneys General with "sample" notices of the Data Breach that suggest the information exposed in the Data Breach is not limited to names, Social Security numbers, and home addresses, and phone numbers, but may also include dates of birth and/or financial account numbers.[7]

25. Defendant admitted in the *Notice of Data Breach*, the letters to the Attorneys General, and the "sample" notices of the Data Breach that an unauthorized party accessed one or more documents that contained sensitive information about Defendant's current and former customers, including names, Social Security numbers, home addresses, and phone numbers and potentially including dates of birth and financial account numbers.

26. In response to the Data Breach, Defendant claims that it "promptly took the Accellion server offline and permanently discontinued use of this file sharing platform. Additionally, we acted immediately to contain the threat and

---

[6] *Id.* at 1-2.

[7] *See* Letter to Attorney General of New Hampshire dated March 12, 2021, a true and correct copy of which is attached hereto as Exhibit 2 ("Ex. 2"); Sample Notice of Data Breach provided to Attorney General of California, a true and correct copy of which is attached hereto as Exhibit 3 ("Ex. 3")

engaged a team of third-party forensic experts to investigate and determine the full scope of this incident."[8] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

27. Plaintiffs' and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

28. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing their PII to be exposed.

Defendant Acquires, Collects and Stores Plaintiffs' and Class Members' PII.

29. Defendant acquired, collected, and stored Plaintiffs' and Class Members' PII.

30. As a condition of providing services to its customers, Defendant

[8] Exs. 1, 3.

requires that its customers entrust Defendant with highly confidential PII.

31. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

32. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

33. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data, especially decade-old data from former customers.

34. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

35. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

36. The Federal Trade Commission ("FTC") defines identity theft as "a

fraud committed or attempted using the identifying information of another person without authority."[9] 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."[10]

37. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

38. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number

[9] 17 C.F.R. § 248.201 (2013).
[10] *Id*.
[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*:

can sell for $5 to $110 on the dark web.[12] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[13]

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

> 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.[14]

40. What is more, it is no easy task to change or cancel a stolen Social

---

https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed March 23, 2021).

[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed March 23, 2021).

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed March 23, 2021).

[14] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed March 23, 2021).

Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

41. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

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

43. This data demands a much higher price on the black market. Martin

[15] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed March 23, 2021).

Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

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

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

46. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result,

[16] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed March 23, 2021).

> studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[17]

47. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members a result.

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

49. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's file servers, amounting to potentially more than one million individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

50. To date, Defendant has offered Plaintiffs and Class Members only two

[17] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last accessed March 23, 2021).

years of identity monitoring through a single provider, Kroll. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

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

Defendant Violated the Gramm-Leach-Bliley Act

52. Defendant is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

53. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

54. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

55. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

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

57. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the

information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

58. Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's vendor's file sharing platform.

59. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on a vendor's file sharing platform and would do so after the customer relationship ended.

60. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing

information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendant violated the Safeguard Rule.

61. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information.

62. Defendant failed to adequately (a) oversee its vendor for the file sharing platform where the Data Breach occurred and (b) require the vendor by contract to protect the security and confidentiality of customer information.

63. As of January 4, 2019, Defendant's "Policies and Procedures" for "Compliance" recognized that the GLBA "prohibits financial institutions from sharing the non-public personal information of consumers with non-affiliated third parties except in certain circumstances."

64. As of January 4, 2019, Defendant further recognized the GLBA required it to (a) "[p]rovide an opt-out notice prior to sharing non-public personal information with non-affiliated third parties" and (b) "[p]rovide customers with a

'reasonable opportunity' to opt out before disclosing non-public personal information about them to non-affiliated third parties."

65. As of January 4, 2019, Defendant admitted that it had not provided Plaintiffs or Class Members an opt-out notice, stating it "does not currently share non-public personal information with non-affiliated third parties; therefore, it is not required to and does not provide an opt-out notice."

66. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members with Defendant's vendor for the file sharing platform without providing Plaintiffs and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

67. Defendant has not informed Plaintiffs and Class Members of the reason Defendant shared the PII of more than 1.4 million individuals with the vendor for the file sharing platform; if this was done to share the PII with yet another non-affiliated third party, Defendant would be further in breach of the GLBA and its own policy and procedures in failing to provide Plaintiffs and Class Members an opt-out notice and a reasonable opportunity to opt out of such disclosure.

Plaintiff Philip Angus's Experience

68. In 2014, Plaintiff Angus obtained a mortgage from Defendant in connection with the purchase of residential real estate. In connection with his

application for a mortgage loan, Mr. Angus provided financial and other highly sensitive information to Defendant. Mr. Angus's last payment to Defendant was in or around October 2015, when Mr. Angus began making payments to a different entity. More than five years after the customer relationship ended, Defendant stored and/or shared some of Mr. Angus's most sensitive (and extremely valuable to cyber criminals and identity thieves) PII on its vendor's file sharing platform, resulting in the exposure of Mr. Angus's PII during the Data Breach.

69. Since January 2021, Mr. Angus has experienced an increase in the volume of "spam" calls he receives, despite being on the "do not call" list.

70. On or around March 15, 2021, Mr. Angus learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Mr. Angus.

71. As a result of learning of the Data Breach, Mr. Angus spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his financial accounts. This time has been lost forever and cannot be recaptured.

72. Additionally, Mr. Angus is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

73. Mr. Angus stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

74. Mr. Angus suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Angus entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

75. Mr. Angus suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

76. Mr. Angus has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and Social Security number being placed in the hands of unauthorized third-parties and possibly criminals.

77. Mr. Angus has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Mark Wiedder's Experience

78. In approximately 2011, Plaintiff Wiedder refinanced his residential mortgage loan using Defendant's services. In connection with his application, Mr. Wiedder provided financial and other highly sensitive information to Defendant, including his Social Security number.

79. On or about March 5, 2021, Mr. Wiedder learned of the Data Breach via an email from Flagstar. On or about March 15, 2021, Mr. Wiedder received Flagstar's *Notice of Data Breach* that informed Mr. Wiedder that his name and Social Security number had been compromised.

80. On or about March 18, 2021, Mr. Wiedder's debit card was used by an unauthorized third party to make unauthorized purchases for a total of $96.00. Mr. Wiedder's credit union has not reimbursed him for these charges at this point.

81. Moreover, since January 2021, Mr. Wiedder and his spouse have experienced an increase in the volume of "spam" calls they receive.

82. As a result of learning of the Data Breach and the subsequent fraudulent charges, Mr. Wiedder spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the news reports of the Data Breach, exploring credit monitoring and identity theft insurance options, self-monitoring his financial accounts, filing an identity theft affidavit with a government agency, signing up for Defendant's complimentary credit

monitoring services, and monitoring those services on a regular basis. This time has been lost forever and cannot be recaptured.

83. Additionally, Mr. Wiedder is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

84. Mr. Wiedder stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

85. Mr. Wiedder suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Wiedder entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

86. Mr. Wiedder suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

87. Mr. Wiedder has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security number, in combination with his name and Social Security number being placed in the hands of unauthorized third-parties and possibly criminals.

88. Mr. Wiedder has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

89. Plaintiffs bring this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

90. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose PII Defendant stored and/or shared using the file sharing platform referenced in Defendant's correspondence to Plaintiff Angus dated March 15, 2021 and which was exposed to an unauthorized party as a result of the data breach referenced in Defendant's correspondence to Plaintiff Angus dated March 15, 2021 (the "Nationwide Class").

91. The Florida Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in Florida whose PII Defendant stored and/or shared using the file sharing platform referenced in Defendant's correspondence to Plaintiff Angus dated March 15, 2021 and which was exposed to an unauthorized party as a result of the data breach referenced in Defendant's correspondence to Plaintiff Angus dated March 15, 2021 (the "Florida Class").

92. Excluded from the Classes are the following individuals and/or

entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

93. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

94. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") is so numerous that joinder of all members is impracticable. Defendant reported to the Attorney General of Maine that more than 1.4 million individuals were affected by the Data Breach.

95. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;

b. Whether Defendant had a duty not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

96. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

97. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members, and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

98. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages

they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

99. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

100. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of

each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

101. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

102. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

103. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to act unlawfully as set forth in this Complaint.

104. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

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

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

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

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendant failed to implement and maintain reasonable

security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,

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

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

106. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 105.

107. As a condition of being customers of Defendant, Defendant's current and former customers were obligated to provide Defendant with certain PII, including their names, Social Security numbers, home addresses, phone numbers, and dates of birth.

108. Plaintiffs and the Nationwide Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

109. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

110. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

111. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

112. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

113. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

114. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Plaintiffs and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of being customers of Defendant.

115. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

116. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

118. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to

comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

119. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

120. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

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

122. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

123. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

124. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry

protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

125. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

126. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

127. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former customers' PII.

128. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former customers' PII it was no longer required to retain pursuant to regulations.

129. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

130. But for Defendant's wrongful and negligent breach of duties owed to

Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

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

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

133. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Nationwide Class.

134. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

135. Defendant's duty to use reasonable security measures also arose under the GLBA, under which Defendant was required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

136. Defendant violated the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule by (a) failing to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing and/or sharing that PII on Defendant's vendor's file sharing platform, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on a vendor's file sharing platform and would do so after the customer relationship ended, (c) failing to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information, (d) failed to adequately (i) oversee its vendor for the file sharing platform where the Data Breach occurred and (ii) require the vendor by contract to protect the security and confidentiality of customer information, and (e) failing to send opt-out notices and afford a reasonable opportunity to opt out of disclosures before sharing the PII of more than 1.4 million individuals with one or

more non-affiliated third parties.

137. Defendant's violation of the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule constitutes negligence *per se*.

138. Plaintiffs and the Nationwide Class are within the class of persons that the FTC Act and the GLBA were intended to protect.

139. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Nationwide Class. The GLBA, with its Privacy Rule, Regulation P, and Safeguards Rule, was similarly intended to guard against harms such as the harm that occurred as a result of the Data Breach.

140. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity

addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

141. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

142. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so

long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

143. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 105.

144. Defendant required Plaintiffs and the Nationwide Class to provide their personal information, including names, Social Security numbers, home addresses, phone numbers, and other personal information, as a condition of being customers of Defendant. Defendant may have also required Plaintiffs and the Nationwide Class to provide their dates of birth and financial account information as a condition of being customers of Defendant.

145. As a condition of being customers of Defendant, Plaintiffs and the Nationwide Class provided their personal and financial information. In so doing, Plaintiffs and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

146. Plaintiffs and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

147. Defendant breached the implied contracts it made with Plaintiffs and the Nationwide Class by failing to safeguard and protect their personal and financial information and by failing to provide timely and accurate notice to them that personal and financial information was compromised as a result of the data breach.

148. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

149. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 105.

150. Plaintiffs and the Nationwide Class had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

151. Defendant owed a duty to its current and former customers, including Plaintiffs and the Nationwide Class, to keep their PII contained as a part thereof, confidential.

152. Defendant failed to protect and released to unknown and unauthorized third parties the PII of Plaintiffs and the Nationwide Class.

153. Defendant allowed unauthorized and unknown third parties access to and examination of the PII of Plaintiffs and the Nationwide Class, by way of Defendant's failure to protect the PII.

154. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Nationwide Class is highly offensive to a reasonable person.

155. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and the Nationwide Class disclosed their PII to

Defendant as part of the current and former customers' relationship with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

156. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs' and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

157. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

158. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and the Nationwide Class.

159. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiffs and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiffs and the Nationwide Class to suffer damages.

160. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to

Plaintiffs and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Nationwide Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

161. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 105.

162. At all times during Plaintiffs' and the Nationwide Class's interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and the Nationwide Class's PII that Plaintiffs and the Nationwide Class provided to Defendant.

163. As alleged herein and above, Defendant's relationship with Plaintiffs and the Nationwide Class was governed by terms and expectations that Plaintiffs' and the Nationwide Class's PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

164. Plaintiffs and the Nationwide Class provided their PII to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

165. Plaintiffs and the Nationwide Class also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

166. Defendant voluntarily received in confidence the PII of Plaintiffs and the Nationwide Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

167. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiffs and the Nationwide Class was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Nationwide Class's confidence, and without their express permission.

168. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and the Nationwide Class have suffered damages.

169. But for Defendant's disclosure of Plaintiffs' and the Nationwide Class's PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Nationwide Class's PII as well as the resulting damages.

170. The injury and harm Plaintiffs and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Nationwide Class's PII. Defendant knew or should have known

its methods of accepting and securing Plaintiffs' and the Nationwide Class's PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Nationwide Class's PII.

171. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Nationwide Class, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of current and former customers; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII

compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

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

COUNT V
Violation of the Florida Deceptive and Unfair Trade Practices Act, (Fla. Stat. §§ 501.201, *et seq.*)
(On Behalf of Plaintiff Angus and the Florida Class)

173. Plaintiff Angus and the Florida Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 105.

174. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained the PII of Plaintiff Angus and the Florida Class through advertising, soliciting, providing, offering, and/or distributing goods and services to Plaintiff Angus and the Florida Class and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

175. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard PII;

b. failure to make only authorized disclosures of current and former customers' PII;

c. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft; and

d. failure to timely and accurately disclose the Data Breach to Plaintiff Angus and the Florida Class.

176. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former customers.

177. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former customers that it did not follow industry best practices for the collection, use, and storage of PII.

178. As a direct and proximate result of Defendant's conduct, Plaintiff Angus and the Florida Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration

services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

179. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff Angus and the Florida Class have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

180. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff Angus and the Florida Class are entitled to damages as well as injunctive relief, including, but not limited to:

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

f. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

g. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

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

i. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner PII not necessary for its provisions of services;

j. Ordering that Defendant conduct regular database scanning and securing checks;

k. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

l. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members,

request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and the Florida Class and appointing Plaintiffs and their Counsel to represent each such Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

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

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

iii. requiring Defendant to delete, destroy, and purge the personal

identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

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

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

viii. requiring Defendant to audit, test, and train its security personnel

regarding any new or modified procedures;

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

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs

discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report

to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: March 24, 2021

Respectfully Submitted,

By: s/ *Michael N. Hanna*
MICHAEL N. HANNA (P81462)
MORGAN & MORGAN, P.A.
Attorney for Plaintiffs
2000 Town Center
Suite 1900
Southfield, MI 48075
Tel: (313) 251-1399
mhanna@forthepeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

M. ANDERSON BERRY
(Pro Hac Vice application forthcoming)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com

Attorneys for Plaintiffs and the Putative Class

THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

PHILIP ANGUS and **MARK WIEDDER**, on behalf of themselves and all others similarly situated, Plaintiffs, vs. **FLAGSTAR BANK, FSB**, a Michigan-based federally chartered stock savings bank, Defendant.	Case No.:

INDEX OF EXHIIBTS

Exhibit 1 - Notice of Data Breach

Exhibit 2 - Letter to Attorney General of New Hampshire dated March 12, 2021

Exhibit 3 - Sample Notice of Data Breach provided to Attorney General of California

Flagstar Bank

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

March 15, 2021

Philip Angus
[redacted]

Notice of Data Breach

Dear Philip Angus,

Flagstar Bank respects the privacy of your personal information, which is why we are writing to let you know about a recent security incident. Because the privacy and security of the personal information we maintain is of the utmost importance to us, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021 that the platform had a vulnerability that was exploited by an unauthorized party. Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform – and that we are one of numerous Accellion clients who were impacted.

Flagstar remains fully operational and other parts of our IT infrastructure outside of the Accellion platform were not impacted. Importantly, the Accellion platform was segmented from the rest of our network, and our core banking and mortgage systems were not affected.

What We Are Doing.

Upon learning of the vulnerability, Flagstar promptly took the Accellion server offline and permanently discontinued use of this file sharing platform. Additionally, we acted immediately to contain the threat and engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. As part of our investigation, we have also notified law enforcement.

What Information Was Involved?

On March 6, 2021, we determined that one or more of the documents removed from the Accellion platform contained your Social Security Number, First Name, Last Name, Phone Number, Address.

What You Can Do.

Out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
155 NORTH WACKER DRIVE
CHICAGO, ILLINOIS 60606-1720

TEL: (312) 407-0700
FAX: (312) 407-0411
www.skadden.com

FIRM/AFFILIATE OFFICES
BOSTON
HOUSTON
LOS ANGELES
NEW YORK
PALO ALTO
WASHINGTON, D.C.
WILMINGTON
BEIJING
BRUSSELS
FRANKFURT
HONG KONG
LONDON
MOSCOW
MUNICH
PARIS
SÃO PAULO
SEOUL
SHANGHAI
SINGAPORE
TOKYO
TORONTO

CONFIDENTIAL

March 12, 2021

Via First Class Mail and
Email attorneygeneral@doj.nh.gov

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Flagstar - Accellion Breach

Dear Attorney General:

We write to inform you that Flagstar Bank, FSB ("Flagstar" or "the Company"), 5151 Corporate Drive, Troy, Michigan 48098, will be sending notices to New Hampshire residents advising them of a data breach incident involving Accellion, a vendor that provided a third-party file sharing platform used by Flagstar.

On January 22, 2021, Accellion informed Flagstar that the platform had a vulnerability, which prompted Flagstar to discontinue its use of the platform. Unfortunately, Flagstar subsequently learned on January 24, 2021, that an unauthorized party was able to access some of Flagstar's information on the Accellion platform—and that the Company was one of numerous Accellion clients that were impacted. During its investigation of the breach, Flagstar further learned that the personal information of consumers, including name, address, Social Security Number/tax ID number, date of birth, and/or financial account number without any password or security code that may have provided access to the account, may have been accessed by the unauthorized party. Following a

detailed review of the affected systems, Flagstar determined that 3,755 New Hampshire residents were affected by the incident.[1]

Accellion informed Flagstar that it has reported the matter to law enforcement and Flagstar also notified law enforcement. Following the incident, Flagstar has taken steps to strengthen the security of its systems—such as terminating its use of the Accellion platform involved in the incident and transitioning to another cloud-based product, deploying additional detection and response tools across the Company's network for an added layer of visibility, and taking other measures to harden the Company's cybersecurity defenses—and will take further steps as appropriate to safeguard such information. For the convenience of New Hampshire's impacted residents, Flagstar has arranged to make credit monitoring and identity repair services available to them at no cost for two years.

The formal notice will be sent to the affected residents via first-class U.S. Mail beginning on March 15, 2021. A copy of the consumer notice template is attached. Please contact me if you have any questions.

Sincerely,

William E. Ridgeway
Counsel to Flagstar Bank, FSB
155 N. Wacker Dr.
Chicago, IL 60606
William.Ridgway@skadden.com

Enclosure

[1] Although Flagstar continues to investigate the incident, the Company wishes to provide notice to the affected individuals as soon as possible. Consequently, this number may not be final. In the event Flagstar identifies additional affected customers in New Hampshire, we will provide a supplemental notice as soon as practicable.

Flagstar® Bank

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Flagstar Bank respects the privacy of your personal information, which is why we are writing to let you know about a recent security incident. Because the privacy and security of the personal information we maintain is of the utmost importance to us, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021 that the platform had a vulnerability that was exploited by an unauthorized party. Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform – and that we are one of numerous Accellion clients who were impacted.

Flagstar remains fully operational and other parts of our IT infrastructure outside of the Accellion platform were not impacted. Importantly, the Accellion platform was segmented from the rest of our network, and our core banking and mortgage systems were not affected.

What We Are Doing.

Upon learning of the vulnerability, Flagstar promptly took the Accellion server offline and permanently discontinued use of this file sharing platform. Additionally, we acted immediately to contain the threat and engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. As part of our investigation, we have also notified law enforcement.

What Information Was Involved?

On March 6, 2021, we determined that one or more of the documents removed from the Accellion platform contained your <<b2b_text_1(DataElements)>>.

What You Can Do.

Out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Please review the attachment to this letter, entitled "Steps You Can Take to Further Protect Your Information," for further information. The attachment also includes the toll-free telephone numbers and addresses of the three major credit reporting agencies. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely apologize for any inconvenience this may have caused you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-855-907-0446. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday between 9:00 AM to 6:30 PM Eastern Time.

Visit flagstar.com/protect for further ways you can protect yourself, including reviewing accounts, checking your credit report and additional best practices to keep your data secure.

Sincerely,

Zahira Gonzalvo, Chief Information Security and Privacy Officer
Flagstar Bank
5151 Corporate Drive ▪ Troy, MI 48098

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

- **Activate Identity Monitoring Services**

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 1, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

You've been provided with access to the following services* from Kroll:

Credit Monitoring

You will receive alerts when there are changes to your credit data – for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

* Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements, from us and others, and monitoring your credit reports closely. If you detect any suspicious activity on any account or have reason to believe your information is being misused, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and the Federal Trade Commission ("FTC"). If you file an identity theft report with your local police department, you should ask for and are entitled to receive a copy of the police report. Some creditors may ask for the information contained in the report.

You may be able to obtain information from your state's attorney general on the steps you can take to avoid identity theft. Contact information for your state's attorney general is available at http://www.naag.org/naag/attorneys-general/whos-my-ag.php.

To file a complaint with the FTC, go to https://www.identitytheft.gov/ or call (877) ID-THEFT (877-438-4338), a toll- free number. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies. Additional contact information for the FTC is provided below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222

For information from the FTC on how federal law limits your liability for unauthorized charges to certain accounts, please visit http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

- **Review a Copy of Your Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting https://www.annualcreditreport.com/index.action, calling toll-free (877) 322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies.

Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	*Experian*	*TransUnion*
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Stolen account information is sometimes held for future use or shared among a group of thieves at different times. Checking your credit report periodically can help you spot problems and address them quickly.

- **Place a Fraud Alert on Your Credit File**

You may want to consider placing a fraud alert on your credit reports. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com/index.action.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may contact any one of the three nationwide credit reporting companies below to place a fraud alert on your files. We recommend that you contact one of the credit reporting companies by phone or online to find out the specific requirements and expedite this process. As soon as one credit reporting company confirms your fraud alert, the others are notified to place fraud alerts. After your fraud alert request, all three credit reporting companies will send you one free credit report for your review.

Equifax	*Experian*	*TransUnion*
(800) 525-6285 www.fraudalerts.equifax.com P. O. Box 105788 Atlanta, GA 30348	(888) 397-3742 www.experian.com/fraud/center P. O. Box 9554 Allen, TX 75013	(800) 680-7289 www.transunion.com/personal credit/ credit disputes/fraud-alerts.page P. O. Box 6790 Fullerton, CA 92834-6790

- **Place a Security Freeze on Your Credit File**

You also have the right to place a security freeze on your credit file. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit file, you need to separately contact each of the three nationwide credit reporting companies. A security freeze can be placed on your credit file at no cost to you. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. We recommend that you contact the credit reporting companies, identified above, by phone or online to find out their specific requirements and expedite this process.

- **Best Practices on Helping to Keep Your Data Secure**

  - Do not share personal information over the phone, through the mail, or over the internet unless you initiated the contact or know the person you are dealing with. If someone contacts you unexpectedly and asks for your personal information, even if it is a company you regularly conduct business with, call the company back directly using the published company phone number to verify the request is legitimate before providing any data;
  - Choose PINs and passwords that would be difficult to guess and avoid using easily identifiable information such as your mother's maiden name, birth dates, the last four digits of your Social Security number, or phone numbers. Also, avoid using the same password for online banking that you use for other accounts. Your online banking password should be unique to that account only;
  - Pay attention to billing cycles and account statements and contact us if you don't receive a monthly bill or statement since identity thieves often divert account documentation;
  - Be careful about where and how you conduct financial transactions, for example, don't use an unsecured Wi-Fi network because someone might be able to access the information you are transmitting or viewing.
  - Monitor your accounts regularly for fraudulent transactions. Review payees for online bill payments and Zelle contacts, if applicable. Sign up for account alerts through online banking for certain actions, such as an address or password change. Notify Flagstar Bank immediately if you find any suspicious activity on your account.

- **Research Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit http://www.consumer.ftc.gov/features/feature-0014-identity-theft or call (877) ID-THEFT (877-438-4338).

Flagstar® Bank

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Flagstar Bank respects the privacy of your personal information, which is why we are writing to let you know about a recent security incident. Because the privacy and security of the personal information we maintain is of the utmost importance to us, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar on January 22, 2021 that the platform had a vulnerability that was exploited by an unauthorized party. Flagstar permanently discontinued use of this file sharing platform. Unfortunately, we have learned that the unauthorized party was able to access some of Flagstar's information on the Accellion platform – and that we are one of numerous Accellion clients who were impacted.

Flagstar remains fully operational and other parts of our IT infrastructure outside of the Accellion platform were not impacted. Importantly, the Accellion platform was segmented from the rest of our network, and our core banking and mortgage systems were not affected.

What We Are Doing.

Upon learning of the vulnerability, Flagstar promptly took the Accellion server offline and permanently discontinued use of this file sharing platform. Additionally, we acted immediately to contain the threat and engaged a team of third-party forensic experts to investigate and determine the full scope of this incident. As part of our investigation, we have also notified law enforcement.

What Information Was Involved?

On March 6, 2021, we determined that one or more of the documents removed from the Accellion platform contained your <<b2b_text_1(DataElements)>>.

What You Can Do.

Out of an abundance of caution we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Please review the attachment to this letter, entitled "Steps You Can Take to Further Protect Your Information," for further information. The attachment also includes the toll-free telephone numbers and addresses of the three major credit reporting agencies. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

We sincerely apologize for any inconvenience this may have caused you. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 1-855-907-0446. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday between 9:00 AM to 6:30 PM Eastern Time.

Visit flagstar.com/protect for further ways you can protect yourself, including reviewing accounts, checking your credit report and additional best practices to keep your data secure.

Sincerely,

Zahira Gonzalvo, Chief Information Security and Privacy Officer
Flagstar Bank
5151 Corporate Drive ▪ Troy, MI 48098

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

- **Activate Identity Monitoring Services**

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 1, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

You've been provided with access to the following services* from Kroll:

Credit Monitoring

You will receive alerts when there are changes to your credit data – for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

* Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements, from us and others, and monitoring your credit reports closely. If you detect any suspicious activity on any account or have reason to believe your information is being misused, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and the Federal Trade Commission ("FTC"). If you file an identity theft report with your local police department, you should ask for and are entitled to receive a copy of the police report. Some creditors may ask for the information contained in the report.

You may be able to obtain information from your state's attorney general on the steps you can take to avoid identity theft. Contact information for your state's attorney general is available at http://www.naag.org/naag/attorneys-general/whos-my-ag.php.

To file a complaint with the FTC, go to https://www.identitytheft.gov/ or call (877) ID-THEFT (877-438-4338), a toll- free number. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies. Additional contact information for the FTC is provided below:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
Telephone: (202) 326-2222

For information from the FTC on how federal law limits your liability for unauthorized charges to certain accounts, please visit http://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards.

- **Review a Copy of Your Credit Report**

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve months by visiting https://www.annualcreditreport.com/index.action, calling toll-free (877) 322-8228, or completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies.

Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	*Experian*	*TransUnion*
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically. Stolen account information is sometimes held for future use or shared among a group of thieves at different times. Checking your credit report periodically can help you spot problems and address them quickly.

- **Place a Fraud Alert on Your Credit File**

You may want to consider placing a fraud alert on your credit reports. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com/index.action.

A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. You may contact any one of the three nationwide credit reporting companies below to place a fraud alert on your files. We recommend that you contact one of the credit reporting companies by phone or online to find out the specific requirements and expedite this process. As soon as one credit reporting company confirms your fraud alert, the others are notified to place fraud alerts. After your fraud alert request, all three credit reporting companies will send you one free credit report for your review.

Equifax	*Experian*	*TransUnion*
(800) 525-6285 www.fraudalerts.equifax.com P. O. Box 105788 Atlanta, GA 30348	(888) 397-3742 www.experian.com/fraud/center P. O. Box 9554 Allen, TX 75013	(800) 680-7289 www.transunion.com/personal credit/ credit disputes/fraud-alerts.page P. O. Box 6790 Fullerton, CA 92834-6790

- **Place a Security Freeze on Your Credit File**

You also have the right to place a security freeze on your credit file. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. To place a security freeze on your credit file, you need to separately contact each of the three nationwide credit reporting companies. A security freeze can be placed on your credit file at no cost to you. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. We recommend that you contact the credit reporting companies, identified above, by phone or online to find out their specific requirements and expedite this process.

- **Best Practices on Helping to Keep Your Data Secure**

  - Do not share personal information over the phone, through the mail, or over the internet unless you initiated the contact or know the person you are dealing with. If someone contacts you unexpectedly and asks for your personal information, even if it is a company you regularly conduct business with, call the company back directly using the published company phone number to verify the request is legitimate before providing any data;
  - Choose PINs and passwords that would be difficult to guess and avoid using easily identifiable information such as your mother's maiden name, birth dates, the last four digits of your Social Security number, or phone numbers. Also, avoid using the same password for online banking that you use for other accounts. Your online banking password should be unique to that account only;
  - Pay attention to billing cycles and account statements and contact us if you don't receive a monthly bill or statement since identity thieves often divert account documentation;
  - Be careful about where and how you conduct financial transactions, for example, don't use an unsecured Wi-Fi network because someone might be able to access the information you are transmitting or viewing.
  - Monitor your accounts regularly for fraudulent transactions. Review payees for online bill payments and Zelle contacts, if applicable. Sign up for account alerts through online banking for certain actions, such as an address or password change. Notify Flagstar Bank immediately if you find any suspicious activity on your account.

- **Research Additional Free Resources on Identity Theft**

You may wish to review the tips provided by the FTC on how to avoid identity theft. For more information, please visit http://www.consumer.ftc.gov/features/feature-0014-identity-theft or call (877) ID-THEFT (877-438-4338).