UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

ALEXIS and GEORGE COUSINO, Individually and On Behalf of All Others Similarly Situated, Plaintiffs, v. FLAGSTAR BANK, FSB, Defendant.	**Civil Action No.** CLASS ACTION COMPLAINT **JURY TRIAL DEMANDED**

Plaintiffs Alexis and George Cousino ("Plaintiffs"), on behalf of themselves and others similarly situated, bring this class action against Flagstar Bank, FSB ("Flagstar" or the "Defendant"). Plaintiffs make the following allegations, except as to allegations specifically pertaining to Plaintiffs, upon information and belief based upon, *inter alia*, the investigation of counsel and review of public documents.

NATURE OF THE ACTION

1. This is a class action on behalf of the over 1.5 million individuals whose sensitive personal identifying information was compromised in a cybersecurity breach of Flagstar, which was announced on or about June 17, 2022 (the "Flagstar Breach").

2. According to Flagstar's reports of the Flagstar Breach to several state attorneys general, the compromised personal information consisted of names, addresses, Social Security numbers, financial information (e.g. account numbers, credit or debit card numbers), and "other" types of personal identifiable information.

3. Flagstar failed to adequately protect consumers' sensitive personal identifying information. Lack of proper safeguards provided a means for unauthorized intruders to breach Flagstar's computer network and steal sensitive personal identifying information.

4. Armed with this sensitive personal identifying information, hackers can commit a variety of crimes including, among other things, taking out loans in another person's name; opening new financial accounts in another person's name; using the victim's information to obtain government benefits; filing a fraudulent tax return and using the victim's information to obtain a tax refund; obtaining a driver's license or identification card in the victim's name but with another person's picture; or giving false information to police during an arrest.

5. As a result of the Flagstar Breach, Plaintiffs and Class members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now, and in the future, closely monitor their financial accounts to guard against identity theft. Plaintiffs and Class members may be faced with fraudulently incurred debt. Plaintiffs and Class members may also incur out of

pocket costs for, among other things, obtaining credit reports, credit freezes, or other protective measures to deter or detect identity theft.

6. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly-situated individuals and entities whose sensitive personal identifying information was accessed during the Flagstar Breach.

7. Plaintiffs seek remedies including, but not limited to, reimbursement of out-of-pocket losses, further credit monitoring services with accompanying identity theft insurance, and improved data security.

PARTIES

8. Plaintiffs Alexis and George Cousino are citizens of Michigan who reside in Flat Rock, Michigan.

9. Plaintiffs are Flagstar customers. On or about June 17, 2022, they received letters from Flagstar notifying them that their personal information had been compromised.

10. Defendant Flagstar Bank, FSB is a Michigan-based entity with its principal place of business at 5151 Corporate Drive, Troy, Michigan 48097. Defendant is a full-service bank that provides commercial, small business, and consumer banking services, as well as home loans. Flagstar serves customers throughout the United States.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2). If a class is certified in this action, the amount in controversy will exceed $5,000,000.00, exclusive of interest and costs. There are more than 100 members in the proposed class, and at least one member of the proposed class is a citizen of a state different from Flagstar.

12. This Court has personal jurisdiction over Flagstar because Flagstar has its principal place of business in Michigan and conducts substantial business in this District.

13. Venue is also proper within this District because, pursuant to 28 U.S.C. § 1391(b)(1) & (c)(2), Flagstar is deemed to reside in this District since it is subject to personal jurisdiction in this District. Finally, venue is proper in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District.

SUBSTANTIVE ALLEGATIONS

THE FLAGSTAR BREACH

14. On or about June 17, 2022, Flagstar notified the Maine Attorney General's Office that it had experienced a cybersecurity breach between December 3, 2021 and December 4, 2021 that included customers' names or other personal

identifying information in combination with Social Security numbers.[1] Flagstar reported that the breach had been discovered on June 2, 2022, and that 1,547,169 individuals were affected.

15. Flagstar further reported that affected individuals were sent a written notification of the breach on June 17, 2022 and that Flagstar would offer affected individuals two years of credit monitoring and identity repair services through Kroll.

16. On or about June 20, 2022, Flagstar notified the Texas Attorney General's Office that it had suffered the Flagstar Breach. Flagstar's notification to the Texas Attorney General revealed that names, addresses, Social Security numbers, financial information, and "other" information had been affected by the Flagstar Breach.[2]

17. Flagstar informed multiple media outlets that it had learned of the breach during December 2021, providing a statement to *CNET* that it had detected the intrusion "right away," but had delayed disclosing the breach until it had

[1] Office of the Maine Attorney General, *Data Breach Notifications*, Flagstar Bank, FSB (June 17, 2022), https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml. (Last reviewed on July 8, 2022)

[2] Ken Paxton Attorney General of Texas, *Data Security Breach Reports*, Flagstar Bank, FSB (June 20, 2022), https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage. (Last reviewed on July 8, 2022)

completed its investigation.[3] Flagstar also admitted to *PC Mag* that it "detected and contained the incident in December 2021."[4]

18. Despite knowing about the Flagstar Breach in December 2021, Flagstar did not notify customers whose personal information had been compromised until Flagstar sent a letter to affected individuals on or about June 17, 2022.

19. Further, the Flagstar Breach was not the first time Flagstar customer data was the subject of a cybersecurity breach. In January 2021, hackers gained unauthorized access to Flagstar customer names, Social Security numbers, and home addresses through a breach of third-party vendor Accellion's computer systems.[5] The January 2021 breach put Flagstar on notice that its systems were likely to be targeted by hackers seeking to obtain personal identifying information. Despite this knowledge, Flagstar failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' personal information.

---

[3] Bree Fowler, *Social Security Numbers Stolen in Flagstar Bank Data Breach*, CNET (June 23, 2022, 8:03 AM), https://www.cnet.com/tech/services-and-software/social-security-numbers-stolen-in-flagstar-bank-data-breach/. (Last reviewed on July 8, 2022)

[4] Matthew Humphries, *Flagstar Bank Was Hacked in December, Over 1.5 Million Customers Impacted*, PC MAG (June 22, 2022), https://www.pcmag.com/news/flagstar-bank-was-hacked-but-didnt-realize-for-months. (Last reviewed on July 8, 2022)

[5] Penny Crosman, *Flagstar's data breach, and what banks can learn from it*, American Banker (Mar. 15, 2021, 3:34 PM), https://www.americanbanker.com/news/flagstars-data-breach-and-what-banks-can-learn-from-it. (Last reviewed on July 8, 2022)

20. Despite this prior cybersecurity breach, Flagstar failed to adopt adequate protective measures to ensure that consumers' sensitive personal identifying information would not be improperly accessed.

21. As a result of Flagstar's inadequate measures, sensitive personal identifying information relating to at least 1.5 million individuals was obtained from Flagstar's computer network.

22. As a result of Defendant's failure to keep their personal identifying information from unauthorized access, Plaintiffs and Class members are in imminent, immediate, and continuingly increased risk of harm from fraud and identity theft.

23. Plaintiffs and Class members face a present and substantial risk of out-of-pocket fraud losses such as loans opened in their names, government benefits fraud, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

24. Additionally, Plaintiffs and Class members face a present and substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their personal identifying information.

25. As a condition of providing services to its customers, Defendant requires that its customers entrust Defendant with highly confidential personal information.

26. By obtaining, collecting, and storing the Plaintiffs' and Class members' personal information, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting the personal information from disclosure.

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

28. Defendant's negligence in safeguarding Plaintiffs' and Class members' personal information is further exacerbated by the data breach it experienced in January of 2021.

29. Despite the Defendant's recent previous data breach and the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the personal information of Plaintiffs and Class members from being compromised.

Plaintiffs Alexis Cousino and George Cousino

30. Plaintiffs Alexis Cousino and George Cousino are current Flagstar customers. They have held checking and savings accounts with Flagstar for about ten years.

31. By letters dated June 17, 2022, Flagstar notified each Plaintiff of a "recent security incident" that "involved unauthorized access to [Flagstar's] network." Flagstar's letters notified Plaintiffs that on June 2, 2022, Flagstar had discovered that "certain impacted files containing [their] personal information were accessed and/acquired from [Flagstar's] network between December 3, 2021 and December 4, 2021."

32. Flagstar's letter to Alexis Cousinos also explained that "[o]n June 2, 2022, [Flagstar] determined that one or more of the impacted files contained [her] Social Security number, name, and phone number."

33. Flagstar's letter to George Cousinos also explained that "[o]n June 2, 2022, [Flagstar] determined that one or more of the impacted files contained [his] Social Security number, account/loan number, name, and financial institution name."

FLAGSTAR'S POST-BREACH ACTIONS ARE INADEQUATE

34. In the wake of the Flagstar Breach, Defendant has offered inadequate services. Flagstar is offering identify theft monitoring, including credit monitoring, fraud consultation, and identity theft restoration. Defendant places the burden on Plaintiffs and class members by requiring them to expend the time to enroll in these services, instead of automatically enrolling all those impacted by the Flagstar Breach.

35. Moreover, Flagstar is only offering identity monitoring services for two years, even though the ramifications of personal identifying theft can extend far beyond two years.

36. Flagstar has taken minimal steps to notify customers of the breach. On information and belief, on or around June 17, 2022—over six months after the Flagstar Breach occurred—Flagstar sent a short letter to certain customers notifying them that the breached data included their personal information and posted a terse notification on its website, stating:

> How to Protect Your Information: June 17, 2022
> In December 2021, Flagstar experienced a cyber incident that involved unauthorized access to our network. We want to take a moment to detail what happened, what this means for you, and how you can protect your information.
>
> What happened?
> Upon learning of the incident, we promptly activated our incident response plan, engaged external cybersecurity professionals experienced in handling these types of incidents, and reported the matter to federal law enforcement. We continue to operate all services normally.
>
> Since then, we have taken several measures to toughen our information security. We now believe we have strengthened processes and systems in a way that should reduce our cyber vulnerabilities in the future.
>
> What is Flagstar doing?
> On June 2, 2022, we concluded an extensive forensic investigation and manual document review. We are in the process of notifying individuals who may have been

> impacted directly via U.S. Mail to extend complimentary credit monitoring services.
>
> For those impacted, we have no evidence that any of your information has been misused. Nevertheless, 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.
>
> If you have already activated identity monitoring services through Kroll offered to you previously by Flagstar, we are offering an extension of your services for an additional two years. To enroll in the extension, please call (855) 503-3384 and a representative will assist you with the extension.
>
> Flagstar has also established a call center dedicated to handling inquiries related to this incident and to help impacted individuals take advantage of their identity protection services, which can be reached at (855) 503-3384 between the hours of 9:00am – 6:30pm ET, Monday through Friday. If you are not an impacted individual, but you have questions about how to keep your information safe, please read the following article which provides helpful tips and guidance.[6]

CLASS ACTION ALLEGATIONS

37. Plaintiffs bring this class action pursuant to Fed. R. Civ. P. 23 on behalf of the following class and sub-class:

> All individuals and entities in the United States whose personal identifying information was accessed in the cybersecurity breach announced by Flagstar on or about June 17, 2022 (the "Nationwide Class"); and

[6] Customer Data Information Center, *How to Protect Your Information: June 17, 2022*, Flagstar Bank (June 17, 2022), https://www.flagstar.com/customer-support/customer-data-information-center.html. (Last reviewed on July 8, 2022)

> All individuals and entities in Michigan whose personal identifying information was accessed in the cybersecurity breach announced by Flagstar on or about June 17, 2022 (the "Michigan Sub-Class").

38. Excluded from the Nationwide Class and Michigan Sub-Class are Flagstar; any parent, subsidiary, or affiliate of Flagstar or any employees, officers, or directors of Flagstar; legal representatives, successors, or assigns of Flagstar; and any justice, judge, or magistrate judge of the United States who may hear the case, and all persons related to any such judicial officer, as defined in 28 U.S.C. § 455(b).

39. Upon information and belief, the Nationwide Class and Michigan Sub-Class consist of over a million geographically dispersed members, the joinder of whom in one action is impracticable. Disposition of the claims in a class action will provide substantial benefits to both the parties and the Court.

40. The rights of each member of the Nationwide Class and Michigan Sub-Class were violated in a similar fashion based upon Flagstar's uniform wrongful actions and/or inaction.

41. The following questions of law and fact are common to each Class member and predominate over questions that may affect individual Class members:

i. whether Flagstar engaged in the wrongful conduct alleged herein;

ii. whether Flagstar was negligent in collecting, storing, and/or safeguarding the sensitive personal identifying information of the Class members;

iii. whether Flagstar owed a duty to Plaintiffs and Class members to adequately protect their personal information;

iv. whether Flagstar breached its duties to protect the personal information of Plaintiffs and Class members;

v. whether Flagstar knew or should have known that its data security systems and processes were vulnerable to attack;

vi. whether Flagstar's conduct proximately caused damages to Plaintiffs and Class members;

vii. whether Plaintiffs and Class members are entitled to equitable relief including injunctive relief; and

viii. whether the Class members are entitled to compensation, monetary damages, and/or any other services or corrective measures from Flagstar, and, if so, the nature and amount of any such relief.

42. Plaintiffs' claims are typical of the claims of the Nationwide Class and Michigan Sub-Class in that Plaintiffs, like all Class members, had their sensitive personal identifying information compromised in the Flagstar Breach.

43. Plaintiffs are committed to the vigorous prosecution of this action and will fairly and adequately represent and protect the interests of the proposed Nationwide Class and Michigan Sub-Class. Plaintiffs have no interests that are

antagonistic to and/or that conflict with the interests of other putative Class members.

44. Plaintiffs have retained counsel competent and experienced in the prosecution of complex class action litigation.

45. The members of the proposed Nationwide Class and Michigan Sub-Class are readily ascertainable.

46. A class action is superior to all other available methods for the fair and efficient adjudication of the claims of the Nationwide Class and Michigan Sub-Class. Plaintiffs and the Class members have suffered (and continue to suffer) irreparable harm as a result of Flagstar's conduct. The damages suffered by some of the Class members may be relatively small, preventing those Class members from seeking redress on an individual basis for the wrongs alleged herein. Absent a class action, many Class members who suffered damages as a result of the cybersecurity breach of Flagstar will not be adequately compensated.

47. Prosecuting separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Flagstar. Additionally, adjudications with respect to individual Class members, such as adjudication as to injunctive relief, as a practical matter, would be dispositive of the interests of the other Class members not parties

to the individual adjudications or would substantially impair or impede their ability to protect their interests.

COUNT ONE

NEGLIGENCE
(On behalf of the Nationwide Class and Michigan Sub-Class)

48. Plaintiffs reallege and incorporate all allegations set forth in previous paragraphs as if fully set forth herein.

49. Upon coming into possession of the private, sensitive personal information of Plaintiffs and the Class members, Flagstar had (and continues to have) a duty to exercise reasonable care in safeguarding and protecting the information from being compromised and/or stolen. Flagstar's duty arises from the common law, in part because it was reasonably foreseeable to Flagstar that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

50. Flagstar also had a duty to timely disclose to Plaintiffs and Class members that the Flagstar Breach had occurred and that the sensitive personal identifying information of the Class members—including names, addresses, Social Security numbers, and financial account information—had been, or was reasonably believed to be, compromised. Such duty also arises under the common law because it was reasonably foreseeable to Flagstar that a breach of security was likely to occur

under the circumstances, and would cause damages to the Nationwide Class as alleged herein.

51. Flagstar, by and through its above negligent acts and/or omissions, further breached its duties to the Class members by failing to timely disclose to Plaintiffs and Class members that the Flagstar Breach had occurred and that the sensitive personal identifying information of Plaintiffs and the Class members had been compromised.

52. Flagstar also had a duty to put into place, internal policies and procedures designed to detect and prevent the unauthorized dissemination of the Plaintiffs and Class members' sensitive personal identifying information. Such duty also arises under the common law because it was reasonably foreseeable to Flagstar that a breach of security was likely to occur under the circumstances and would cause damages to the Nationwide Class as alleged herein.

53. Flagstar, by and through its above negligent acts and/or omissions, unlawfully breached its duties to the Class members by, inter alia, failing to exercise reasonable care in protecting and safeguarding the Class members' sensitive personal identifying information within its possession, custody, and control.

54. But for Flagstar's negligent and wrongful breach of the duties it owed (and continues to owe) to Plaintiffs and the Class members, the cybersecurity breach

would not have occurred, and Plaintiffs' and the Class members' sensitive personal identifying information would never have been compromised.

55. The Flagstar Breach and the above-described substantial injuries suffered by Plaintiffs and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of Flagstar's negligence.

COUNT TWO

NEGLIGENCE PER SE
(On behalf of the Nationwide Class and Michigan Sub-Class)

56. Plaintiffs reallege and incorporate all allegations set forth in previous paragraphs as if fully set forth herein.

57. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect sensitive personal identifying information.

58. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose

a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

59. The FTC also has published a document entitled "FTC Facts for Business" which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

60. Further, the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

61. By failing to have reasonable data security measures in place, Flagstar engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

62. Flagstar's violation of Section 5 of the FTC Act constitutes negligence per se.

63. The Flagstar Breach and the above-described substantial injuries suffered by Plaintiffs and the Class members as a direct and proximate result of the breach were reasonably foreseeable consequences of Flagstar's negligence *per se*.

WHEREFORE, Plaintiffs, individually and on behalf of the Nationwide Class and Michigan Sub-Class, respectfully request that the Court certify this action as a class action, with Plaintiffs as class representatives and the undersigned counsel as

class counsel, and enter an order of judgment against Flagstar in favor of the Class that, *inter alia*:

A. awards actual damages to fully compensate the Nationwide Class and Michigan Sub-Class for losses sustained as a direct, proximate, and/or producing cause of Flagstar's unlawful conduct;

B. awards pre-judgment and post-judgment interest at the maximum allowable rates;

C. awards appropriate injunctive and equitable relief;

D. awards reasonable attorneys' fees and costs; and

E. orders any further relief that this Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury to the extent permitted by law.

Dated: July 15, 2022

Respectfully submitted,

/s/ E. Powell Miller
E. Powell Miller (P39487)
Sharon S. Almonrode (P33938)
THE MILLER LAW FIRM, P.C.
Miller Building
950 West University Drive, Suite 300
Rochester, MI 48307
Telephone: (248) 841-2200
Fax: (248) 652-2852
epm@millerlawpc.com
ssa@millerlawpc.com

Joseph H. Meltzer
Melissa L. Troutner
Ethan J. Barlieb
KESSLER TOPAZ
MELTZER & CHECK, LLP
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Fax: (610) 667-7056
jmeltzer@ktmc.com
mtroutner@ktmc.com
ebarlieb@ktmc.com

Gretchen Freeman Cappio (P84390)
Ryan P. McDevitt (P84389)
Sydney Read
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
(206) 623-1900
Fax (206) 623-3384
gcappio@kellerrohrback.com
rmcdevitt@kellerrohrback.com
sread@kellerrohrback.com

Attorneys for Plaintiffs Alexis and George Cousino