JS 44 (Rev. 10/20)

CIVIL COVER SHEET

County in which action arose: OAKLAND

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
TANIA GARCIA

(b) County of Residence of First Listed Plaintiff MIDDLESEX COUNTY (NJ)
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Brian Flick, Dann Law, PO Box 6031040, Cleveland, OH 44103 (513)645-3488

DEFENDANTS
FLAGSTAR BANK, F.S.B.

County of Residence of First Listed Defendant OAKLAND
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

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

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ■ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

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

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*
Click here for: Nature of Suit Code Descriptions.

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

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

TORTS

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

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

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

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

PRISONER PETITIONS
Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

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

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

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

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

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

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

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

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

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ■ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

■ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
28 USC 1332(d)(2)
Brief description of cause:
Negligence, Negligent Entrustment, Bailment, Breach of Implied Contract, Unjust Enrichment, N.J.S.A. 56:8-2

VII. REQUESTED IN COMPLAINT:
■ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.
DEMAND $ 5,000,000.00
CHECK YES only if demanded in complaint:
JURY DEMAND: ■ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*:
JUDGE Arthur Tarnow DOCKET NUMBER 2:21-cv-10657

DATE
March 26, 2021

SIGNATURE OF ATTORNEY OF RECORD
/Brian D Flick (OH #0081605)

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

PURSUANT TO LOCAL RULE 83.11

1. Is this a case that has been previously dismissed?

☐ Yes
☒ No

If yes, give the following information:

Court: _____

Case No.: _____

Judge: _____

2. Other than stated above, are there any pending or previously discontinued or dismissed companion cases in this or any other court, including state court? (Companion cases are matters in which it appears substantially similar evidence will be offered or the same or related parties are present and the cases arise out of the same transaction or occurrence.)

☒ Yes
☐ No

If yes, give the following information:

Court: U.S. Dist. Court for EDMI

Case No.: 2:21-cv-10657

Judge: Arthur J. Tarnow

Notes :

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

TANIA GARCIA, **on behalf of herself and all others similarly situated,** **Plaintiff,** **v.** **FLAGSTAR BANK, FSB,** **Defendant.**	Case No. 21-cv-10671 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Tania Garcia ("Plaintiff"), by and through her attorneys, upon personal knowledge as to herself and her own acts and experiences, and upon information and belief as to all other matters, alleges as follows:

NATURE OF THE ACTION

1. Plaintiff brings this Class Action Complaint ("Complaint") against Defendant Flagstar Bank, FSB ("Flagstar" or "Defendant"), individually and on behalf of all others similarly situated based on Defendant's failure to properly safeguard personally identifiable information ("PII") that it stored on and/or shared using its vendor's file sharing platform, including without limitation, full names, Social Security numbers, residential addresses, phone numbers, dates of birth, and/or financial account numbers.

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."[1] Defendant "operate[s] 150 branches in Michigan, Indiana, California, Wisconsin, and

[1] https://www.flagstar.com/about-flagstar.html (last visited 3/26/2021).

Ohio and provide a full complement of products and services for consumers and businesses."[2]

3. Defendant's "mortgage division operates nationally through 103 retail locations and a wholesale network of approximately 2,350 third-party mortgage originators."[3] Defendant is "also a leading servicer and subservicer of mortgage loans—handling recordkeeping for $227 billion in home loans."[4]

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 Plaintiff and Class Members.

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 Plaintiff and Class Members, including, but not limited to, names, Social Security numbers, tax ID numbers, home addresses, phone numbers, dates of birth, and/or financial account numbers.

6. Flagstar was aware and had full knowledge that Accellion's data security on the platform Flagstar used was lax. In fact, prior to the breach, Accellion encouraged its customers to move to a newer and more secure transfer platform.

7. Flagstar did not adequately safeguard Plaintiff's data, and now she and apparently many other individuals are the victims of a significant data breach that will negatively affect them for the rest of their lives.

8. Flagstar is responsible for allowing this data breach through its failure to implement and maintain reasonable safeguards and its failure to comply with industry-standard data security practices.

9. Despite its role in managing so much sensitive and personal information, Flagstar

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

failed to utilize a competent third-party data transfer company when handling and/or transferring sensitive PII, and Flagstar chose to use an outdated and unsecure transfer platform.

10. Flagstar had numerous statutory, regulatory, contractual, and common law obligations, including those based on its affirmative representations to Plaintiff and Class Members, to keep their PII confidential, safe, secure, and protected from unauthorized disclosure or access.

11. Plaintiff and those similarly situated rely upon Flagstar to maintain the security and privacy of the PII entrusted to it; when providing their PII, they reasonably expected and understood that Flagstar would comply with its obligations to keep the information secure and safe from unauthorized access.

12. In this day and age of regular and consistent data security attacks and data breaches, in particular in the financial services industry, Flagstar's data security breach is particularly egregious.

13. As a result of Flagstar's failures, Plaintiff and the Class Members are at a significant risk of identity theft, financial fraud, and/or other identity-theft or fraud, imminently and for years to come.

14. Just as their PII was stolen because of its inherent value in the black market, now the inherent value of Plaintiff's and the Class Members' PII in the legitimate market is significantly and materially decreased.

15. On information and belief, as a result of this massive data breach, at least hundreds of thousands of individuals nationwide have suffered exposure of PII entrusted to Flagstar.

16. In addition, based on Defendant's actions, Plaintiff and the proposed Class have

received services that were and are inferior to those for which they have contracted, and have not been provided the protection and security Flagstar promised when Plaintiff and the proposed Class entrusted Flagstar with their PII.

17. Plaintiff and members of the proposed Class have suffered actual and imminent injuries as a direct result of the data breach. The injuries suffered by Plaintiff and the proposed Class as a direct result of the data breach include: (a) theft of their personal data; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the consequences of the data breach and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach; (d) the imminent injury arising from potential fraud and identity theft posed by their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (e) damages to and diminution in value of their personal data entrusted to Flagstar and with the mutual understanding that Flagstar would safeguard Plaintiff's and Class Members' personal data against theft and not allow access and misuse of their personal data by others; (f) the reasonable value of the PII entrusted to Flagstar; and (g) the continued risk to their personal data, which remains in the possession of Flagstar and which is subject to further breaches so long as Flagstar fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' personal data in its possession.

18. Plaintiff seeks to remedy these harms, and prevent their future occurrence, on behalf of herself and all similarly situated persons whose personal data was compromised and stolen as a result of the data breach.

19. Accordingly, Plaintiff, on behalf of herself and other members of the Class, asserts claims under the New Jersey Consumer Fraud Act and for breach of implied contract,

negligence, negligent entrustment, bailment, and unjust enrichment, and seeks injunctive relief, declaratory relief, monetary damages, and all other relief as authorized in equity or by law.

THE PARTIES

Plaintiff Tania Garcia

20. Plaintiff Tania Garcia is a resident of Jamesburg, NJ and the owner of real estate located at 1 William Street, Jamesburg, NJ 08831 (the "Garcia Property").

21. On May 10, 2016 Plaintiff took out a mortgage on the Garcia property which Defendant Flagstar Bank, F.S.B. began servicing as of November 9, 2018.

22. In late January 2021, Plaintiff received a notice from her Credit Karma account regarding a potential data breach in January 2021. On or around March 22, 2021, Plaintiff learned of the Data Breach and started to piece together that the Credit Karma alert was related to the Flagstar Data Breach.

23. As a result of learning of the Data Breach, Plaintiff has spent time dealing with the consequences of the Data Breach which includes time spent monitoring news reports to verify the legitimacy of the reports of the Breach, spending time daily checking her credit karma, self-monitoring her financial accounts, and reviewing various email communications she has received since February 1, 2021 from Apple regarding multiple attempted sign-in attempts using her Apple ID.

24. Plaintiff entrusted Flagstar with her PII, including but not limited to her full name, Social Security number, tax ID number, residential addresses, phone number, date of birth, and financial account numbers with the reasonable expectation and understanding that Flagstar would take, at a minimum, industry-standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data

security incidents related to her.

25. Since learning about the breach, Plaintiff has suffered and continues to suffer emotional anguish and distress, including but not limited to fear and anxiety related to the breach of her sensitive personal and financial data.

Defendant Flagstar

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

27. Flagstar entrusted Accellion, Inc. to hold and possess the PII entrusted to Flagstar. Accellion is a software company that purports to offer secure file-transfer to its customers. Accellion boasts the security of its "firewall" products that are intended to prevent data breaches: "When employees click the Accellion button, they know it's the safe, secure way to share sensitive information with the outside world."[5]

28. Accellion offers a file-transfer product called "FTA." This self-described "legacy" product is 20 years old[6] and incapable of preventing modern data security threats.

29. For years, Accellion urged that its customers (such as Flagstar) migrate to its newer, more secure product "Kiteworks," which was launched roughly four years ago, yet even though advised to update its security by its own experts Flagstar still failed to maintain adequate security.

JURISDICTION & VENUE

30. This Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving more than 100 putative Class Members and the amount in controversy exceeds $5,000,000, exclusive of interest

[5] https://www.accellion.com/company/ (last visited 3/26/2021).
[6] https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/ (last visited 3/26/2021)..

and costs. Many members of the putative class are citizens of different states thereby satisfying CAFA's minimal diversity requirement.

31. This Court has general personal jurisdiction over Defendant because Defendant is headquartered in this District and Defendant conducts substantial business in Michigan and this District through its headquarters, officers, parents, and affiliates.

32. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conducts substantial business in this District.

FACTUAL ALLEGATIONS

33. Flagstar used Accellion's outdated legacy File Transfer Appliance ("FTA") to transfer the PII of its current and former employees and customers.

34. Accellion's legacy FTA software relied on CentOS 6 to function.

35. In late 2019, CentOS announced it would no longer support CentOS 6 after November 30, 2020.

36. Upon information and belief, the fact that it was no longer supported by CentOS meant that the FTA software would no longer receive expected vulnerability testing and patching.

37. On or about December 25, 2020, Accellion suffered a massive data breach which exposed the sensitive PII of millions of individuals—including Flagstar's employees and customers.

38. The breach occurred after hackers exploited a vulnerability in Accellion's legacy FTA software through traditional SQL injection methodology.

39. As with all financial banking institutions, use of Flagstar's financial services

requires disclosure of PII to Flagstar by its customers.

40. Similarly, as an employer, Flagstar required its employees to provide much of the same sensitive PII as its customers.

41. Flagstar is fully aware of how sensitive the PII it stores and maintains is. It is also aware of how much PII it collects, uses, and maintains from each Plaintiff or Class Member.

42. By requiring the production of, collecting, obtaining, using, and deriving benefits from Plaintiff's and the Class Members' PII, Flagstar assumed certain legal and equitable duties and knew or should have known that it was responsible for the diligent protection of the PII it collected, stored, and shared with Accellion.

Flagstar Knew it Was and Continues to be a Prime Target for Cyberattacks

43. Flagstar knew it was an ideal target for hackers and those with nefarious purposes related to customer and employee data. It processed and saved multiple types and many levels of PII

44. Yet, Flagstar did not follow generally accepted industry standards to protect the sensitive PII entrusted to it.

45. Flagstar processed all of the personal and financial information that it demands from its customers as a financial services and banking institution, such as full names, Social Security numbers, residential addresses, phone numbers, tax ID numbers, dates of birth, and/or financial account information. In doing so, Flagstar relied upon outdated software from Accellion to transfer such data without adequate security measures.

46. The employment of Flagstar's employees similarly required the entrustment of sensitive PII.

47. The seriousness with which Defendant should have taken its data security is

shown by the number of data breaches perpetrated in the financial industry over the last few years.

48. Despite knowledge of the prevalence of financial data breaches, Defendant failed to prioritize its customers and/or employees' data security by implementing reasonable data security measures to detect and prevent unauthorized access to the millions of sensitive data points of its customers and employees.

49. As a highly successful multibillion dollar company, Flagstar had the resources to invest in the necessary data security and protection measures, as it was told to do. Yet, it did not—instead, consciously disregarding the known risks and continuing to use Accellion's outdated legacy technology.

50. Defendant failed to undertake adequate analyses and testing of its own systems, adequate personnel training, and other data security measures to avoid the failures presented to Flagstar's customers and employees in mid-March of 2021, but which occurred in December of 2020.

51. Despite its awareness, Defendant did not take the necessary and required minimal steps to secure Plaintiff's and the Class Members' PII. As a result, hackers breached and stole important PII from at least hundreds of thousands of Flagstar's customers and/or employees.

Flagstar Provided Misleading Information to Plaintiff and the Class Members

52. Flagstar sent letters to certain Class Members that were patently deficient because they failed to disclose the full range of information that may have been compromised in the breach, downplayed the risk its customers and employees face as a result of the breach, and failed to provide customers and employees with important information such as when the breach occurred, details of how the breach occurred, or the number of individuals affected. A sample

copy of the letters were provided to the California Attorney General and is attached hereto as **Exhibit A**.

53. For example, the letters state: "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." This falsely implies that the decision to discontinue Accellion's services was timely and provided a benefit to the customers and employees affected by the breach, when in fact, Flagstar had prior knowledge Accellion's services were deficient yet failed to act, and the decision to discontinue Accellion's services and investigate the breach had absolutely no impact on the vast amounts of data exposed.

54. The letter downplayed the harmful effects to customers and employees of the breach by stating that "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." Regardless of if these statements are true, it does not change the fact that all of the sensitive PII provided to Accellion, which included full names, Social Security numbers, residential addresses, phone numbers, tax ID numbers, dates of birth, and/or financial account information, was accessed by criminals.

Defendant Owed a Duty to Plaintiff and Class Members to Adequately Safeguard Their PII

55. Defendant is aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information), and the value its users place on keeping their PII secure.

56. Defendant owes a duty to Plaintiff and the Class Members to maintain adequate security and to protect the confidentiality of their PII.

57. Defendant owes a further duty to its customers and employees to immediately and accurately notify them of a breach of its systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

The Sort of PII at Issue Here is Particularly Valuable to Hackers

58. Businesses that store sensitive PII are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

59. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that she or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

60. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to

get credit.[7]

61. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiff and Class Members stolen in the Flagstar security breach constitutes a dream for hackers and a nightmare for Plaintiff and the Class. Plaintiff's and Class Members' stolen personal data represents essentially one-stop shopping for identity thieves.

62. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[8] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[9]

63. More recently the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

64. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

---

[7] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited 3/26/2021).

[8] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited 3/26/2021).

[9] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. 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." *Id*.

65. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[10]

66. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. Plaintiff's and Class Members' personal data that was stolen has a high value on both legitimate and black markets.

67. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[11]

68. Individuals rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy – and the amount is considerable.

69. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects,

---

[10] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited 11/13/2020).

[11] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited 11/13/2020).

protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[12] This study was done in 2002, almost twenty years ago. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

70. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

71. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[13] Former and current Flagstar employees and customers whose Social Security numbers have been compromised will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

72. Again, because the information Defendant allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiff and the Class will continue to grow, and Plaintiff and the Class will continue to be at substantial risk for further imminent and future harm.

---

[12] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited 3/26/2021).

[13] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

Flagstar's Post-Breach Activity was Inadequate

73. Personal and financial information can be sold on the black-market almost immediately. As then Illinois Attorney General Lisa Madigan aptly put it, "the second somebody gets your credit or debit card information, it can be a matter of hours or days until it's sold on the black market and someone's starting to make unauthorized transactions."[14] Thus, the compromised information could be used weeks before the receipt of any notification from Flagstar and Flagstar's proposed solutions to the potential fraud are, therefore, woefully deficient.

74. Immediate notice of a security breach is essential to protect people such as Plaintiff and the Class Members. Defendant failed to provide such immediate notice, in fact taking roughly three months to disclose to certain Class Members that there had been a breach, thus further exacerbating the damages sustained by Plaintiff and the Class resulting from the breach. Other Class Members still have not received notice their PII was exposed.

75. Such failure to protect Plaintiff's and the Class Members' PII, and timely notify them of the breach, has significant ramifications. The information stolen allows criminals to commit theft, identity theft, and other types of fraud. Moreover, because many of the data points stolen are persistent—for example, Social Security number, name, and address—as opposed to transitory—criminals who purchase the PII belonging to Plaintiff and the Class Members do not need to use the information to commit fraud immediately. The PII can be used or sold for use years later.

76. Every year, victims of identity theft lose billions of dollars. And reimbursement is only the beginning, as these victims usually spend hours and hours attempting to repair the

[14] Phil Rosenthal, *Just assume your credit and debit card data were hacked*, http://www.chicagotribune.com/business/columnists/ct-data-breach-credit-scam-rosenthal-1001-biz-20140930-column.html#page=1 (last visited 3/26/2021).

impact to their credit, at a minimum.

77. Plaintiff and the Class Members are at constant risk of imminent and future fraud, misuse of their PII, and identity theft for many years in the future as a result of the Defendant's actions and the data breach. They have suffered real and tangible loss, including but not limited to the loss in the inherent value of their PII, the loss of their time as they have had to spend additional time monitoring accounts and activity, and additional economic loss to mitigate the costs of injuries realized as a result of the breach.

CLASS ACTION ALLEGATIONS

78. Plaintiff brings all claims as Class claims under Federal Rule of Civil Procedure 23. The requirements of Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3) are met with respect to the Class defined below.

79. Under Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a national Class action for herself and all members of the following Class of similarly situated persons:

The Nationwide Class

> All individuals whose personally identifiable information was entrusted to Flagstar and was compromised in the December 2020 data breach.

The New Jersey Subclass

> All New Jersey residents whose personally identifiable information was entrusted to Flagstar and was compromised in the December 2020 data breach.

80. Excluded from the Class and Subclass are Defendant; any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendant; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendant. Also excluded are the judges and court personnel in this case and any members of their immediate families.

81. Plaintiff reserves the right to modify and/or amend the Class and Subclass definition, including but not limited to creating additional subclasses, as necessary.

82. Certification of Plaintiff's claims for Class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a Class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

83. All members of the proposed Class are readily ascertainable in that Flagstar has access to addresses and other contact information for all members of the Class, which can be used to provide notice to Class Members.

84. ***Numerosity***. The Class is so numerous that joinder of all members is impracticable. The Class includes at least hundreds of thousands of individuals whose personal data was entrusted to Flagstar and compromised in the Flagstar data security breach.

85. ***Commonality***. There are numerous questions of law and fact common to Plaintiff and the Class, including the following:

whether Defendant engaged in the wrongful conduct alleged in this Complaint;

whether Defendant's conduct was unlawful;

whether Defendant failed to implement and maintain reasonable systems and security procedures and practices to protect customers' and/or employees' personal data;

whether Defendant unreasonably delayed in notifying those affected of the security breach;

whether Defendant owed a duty to Plaintiff and members of the Class to adequately protect their personal data and to provide timely and accurate notice of the Flagstar security breach to Plaintiff and members of the Class;

whether Defendant breached its duties to protect the personal data of Plaintiff and members of the Class by failing to provide adequate data security and failing to provide timely and adequate notice of the Flagstar security breach to Plaintiff and the Class;

whether Defendant's conduct was negligent;

whether Defendant knew or should have known that Accellion's FTA software was vulnerable to attack;

whether Defendant wrongfully or unlawfully failed to inform Plaintiff and members of the Class that it did not ensure that computers and security practices adequate to reasonably safeguard customers' or employees' financial and personal data were used when handling Plaintiff's and the Class Members' personal data;

whether Defendant should have notified the public, Plaintiff, and Class Members immediately upon learning of the security breach;

whether Plaintiff and members of the Class suffered injury, including ascertainable losses, as a result of Defendant's conduct (or failure to act);

whether Defendant breached its duties to Plaintiff and the Class as a bailee of PII entrusted to it and for which Defendant owed a duty to safeguard and of safekeeping;

whether Plaintiff and members of the Class are entitled to recover damages; and

whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or other equitable relief; and

whether Defendant breached its duties to the Subclass under the New Jersey Consumer Fraud Act.

86. ***Typicality***. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class Members, had her personal data compromised, breached and stolen in the Flagstar security breach. Plaintiff and all Class Members were injured through Defendant's uniform misconduct described in this Complaint and assert the same claims for relief.

87. ***Adequacy***. Plaintiff and counsel will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel who are experienced in Class action and complex litigation. Plaintiff has no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

88. ***Predominance***. The questions of law and fact common to Class Members predominate over any questions which may affect only individual members.

89. ***Superiority***. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Moreover, absent a Class action, most Class Members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of Class treatment, Defendant's violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiff and Class Members have been harmed by Defendant's wrongful conduct and/or action. Litigating this action as a Class action will reduce the possibility of repetitious litigation relating to Defendant's conduct and/or inaction. Plaintiff knows of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

90. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

91. Class certification is appropriate under Fed. R. Civ. P. 23(b)(1)(A), in that the prosecution of separate actions by the individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action conserves judicial resources and the parties' resources and protects the rights of each Class Member.

COUNT I — NEGLIGENCE
(On behalf of the Class)

92. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

93. Flagstar owed a duty to Plaintiff and Class Members to safeguard their PII. As

part of this duty, Flagstar was required to retain competent third-party data transfer companies to prevent foreseeable harm to Plaintiff and the Class Members, and therefore had a duty to take reasonable steps to safeguard PII from unauthorized release or theft.

94. In other words, Flagstar was required to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

95. Flagstar's duty included, among other things, designing, maintaining, and testing its security systems to ensure that Plaintiff's and Class Members' PII in its possession was adequately secured and protected.

96. Flagstar further owed a duty to Plaintiff and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts.

97. There is a very close connection between Flagstar's failure to follow reasonable security standards to protect the personal data in its possession and the injury to Plaintiff and the Class. When individuals have their personal information stolen, they are at substantial risk for imminent identity theft, and need to take steps to protect themselves, including, for example, buying credit monitoring services and purchasing or obtaining credit reports to protect themselves from identity theft.

98. If Flagstar had taken reasonable security measures, data thieves would not have been able to take the personal information of Plaintiff and the Class Members. The policy of preventing future harm weighs in favor of finding a special relationship between Flagstar and Plaintiff and the Class. If companies are not held accountable for failing to take reasonable security measures to protect personal data in their possession, they will not take the steps that are

necessary to protect against future security breaches.

99. Flagstar breached its duties by the conduct alleged in the Complaint by, including without limitation, failing to protect the PII in its possession; failing to maintain adequate computer systems and data security practices to safeguard the PII in its possession; failing to utilize adequate, updated, and secure software and related systems to protect the PII in its possession; failing to disclose the material fact that its and its vendor's computer systems and data security practices were inadequate to safeguard the PII from theft; and failing to disclose in a timely and accurate manner to Plaintiff and members of the Class the material fact of the data breach.

100. As a direct and proximate result of Flagstar's failure to exercise reasonable care and use commercially reasonable security measures, the personal data of Flagstar's employees and customers was accessed by ill-intentioned criminals who could and will use the information to commit identity or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

101. As a proximate result of this conduct, Plaintiff and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

COUNT II — NEGLIGENT ENTRUSTMENT
(On behalf of the Class)

102. Plaintiff incorporates by reference all other allegations in the Complaint as if fully

set forth here.

103. Flagstar owed a duty to Plaintiff and the Class to adequately safeguard the PII that it required its employees and customers to provide. Part and parcel with this duty was the duty to only entrust that data to third-party vendors with adequate and reasonable security measures and systems in place to prevent the unauthorized disclosure of such data.

104. Flagstar breached this duty by entrusting Accellion with the sensitive PII of its employees and customers when, as described throughout the Complaint, it knew or should have known that Accellion and Accellion's legacy FTA software was incompetent at preventing such unauthorized disclosure.

105. As a direct and proximate result of Flagstar's failure to exercise reasonable care in whom it entrusted its employees' and customers' sensitive PII to, the personal data of Flagstar's employees and customers was accessed by ill-intentioned criminals who could and will use the information to commit identity theft or financial fraud. Plaintiff and the Class face the imminent, certainly impending and substantially heightened risk of identity theft, fraud and further misuse of their personal data.

106. As a proximate result of this conduct, Plaintiff and the other Class Members suffered damage after the unauthorized data release and will continue to suffer damages in an amount to be proven at trial. Furthermore, Plaintiff and the Class have suffered emotional distress as a result of the breach and have lost time and/or money as a result of past and continued efforts to protect their PII and prevent the unauthorized use of their PII.

COUNT III — BAILMENT
(On behalf of the Class)

107. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

108. Plaintiff and the Class delivered their personal and financial information to Flagstar for the exclusive purpose of obtaining services or employment.

109. The PII is intangible personal property belonging to Plaintiff and the Class Members.

110. In delivering their personal data to Flagstar, Plaintiff and Class Members intended and understood that Flagstar would adequately safeguard their personal data, including by exercising reasonable care in whom it provides its employees' and customers' PII to.

111. Flagstar accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing employment and/or services to Plaintiff and Class Members.

112. A bailment (or deposit) was established for the mutual benefit of the parties.

113. During the bailment (or deposit), Flagstar owed a duty to Plaintiff and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal data as well as a duty to safeguard personal information properly and maintain reasonable security procedures and practices to protect such information. Flagstar breached this duty when it entrusted its employees' and customers' PII to Accellion through the use of Accellion's outdated legacy FTA software, which Flagstar knew or should have known was incapable of providing reasonable security to Flagstar's data.

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

115. As a proximate result of this conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT IV — BREACH OF IMPLIED CONTRACT
(On behalf of the Class)

116. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth here.

117. Plaintiff and the Class delivered their PII to Flagstar as part of the process of obtaining employment or services provided by Flagstar.

118. Plaintiff and members of the Class entered into implied contracts with Flagstar under which Flagstar agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their data had been breached and compromised.

119. In providing such data, Plaintiff and the other members of the Class entered into an implied contract with Flagstar whereby Flagstar became obligated to reasonably safeguard Plaintiff's and the other Class Members' sensitive, non-public information.

120. In delivering their personal data to Flagstar, Plaintiff and Class Members intended and understood that Flagstar would adequately safeguard their personal data.

121. Plaintiff and the Class Members would not have entrusted their PII to Flagstar in the absence of such an implied contract.

122. Flagstar accepted possession of Plaintiff's and Class Members' PII for the purpose of providing services or employment to Plaintiff and Class Members.

123. Had Flagstar disclosed to Plaintiff and members of the Class that it would entrust such data to incompetent third-party vendors that did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and members of the Class would not have provided their PII to Flagstar.

124. Flagstar recognized that its employees' and customers' personal data is highly

sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and members of the Class. For example, the letter Flagstar provided to certain members of the Class states "the privacy and security of the personal information we maintain is of the utmost importance to us…." **Exhibit A**; *see also id.* ("We remain fully committed to maintaining the privacy of personal information in our possession….").

125. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Flagstar.

126. Flagstar breached the implied contract with Plaintiff and the other members of the Class by failing to take reasonable measures to safeguard their data and instead entrusting such data to Accellion through Accellion's outdated and vulnerable legacy FTA software.

127. As a proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT V — UNJUST ENRICHMENT
(On behalf of the Class)

128. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

129. Plaintiff and Class Members conferred a monetary benefit on Flagstar in the form of monies or fees paid for services from Flagstar. Flagstar had knowledge of this benefit when it accepted the money from Plaintiff and the Class Members.

130. The monies or fees paid by the Plaintiff and Class Members were supposed to be used by Flagstar, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and Class Members.

131. Flagstar failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiff and Class Members, instead entrusting such data to Accellion through

Accellion's outdated and vulnerable legacy FTA software, and as a result Plaintiff and the Class overpaid Flagstar as part of the services they purchased.

132. Flagstar failed to disclose to Plaintiff and members of the Class that Accellion's practices and software and systems (which Flagstar chose to utilize) were inadequate to safeguard Plaintiff's and the Class Members PII against theft.

133. Under principles of equity and good conscience, Flagstar should not be permitted to retain the money belonging to Plaintiff and Class Members because Flagstar failed to provide adequate safeguards and security measures to protect Plaintiff's and Class Members' personal and financial information that they paid for but did not receive.

134. Flagstar wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

135. Flagstar's enrichment at the expense of Plaintiff and Class Members is and was unjust.

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

COUNT VI – VIOLATION OF N.J.S.A § 56:8-2, THE CONSUMER FRAUD ACT
(On behalf of the Subclass)

137. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

138. The New Jersey Consumer Fraud Act ("CFA") prohibits:

> The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate.

N.J.S.A. § 56:8-2.

139. The term "unconscionable" under the CFA implies a lack of good faith, honesty in fact and observance of fair dealing.

140. Defendant committed an "unconscionable commercial practice" by failing to use reasonable measures, as interpreted and enforced by the FTC, to protect the PII of Garcia and all subclass Members.

141. Defendant's acts and practices were unconscionable given the nature and amount of PII it stores and the foreseeable consequences of the immense damages that would result to Garcia and all subclass Members by failing to follow reasonable procedures to safeguard PII.

142. The gravity of the harm to members of the Subclass resulting from these unlawful acts and practices outweighed any conceivable reasons, justifications, and/or motives that Defendants had—in this case the desire to save money by not using industry standard practices in protecting the PII entrusted to it—for engaging in such deceptive acts and practices. By committing the acts and practices alleged above, Defendant engaged in unlawful business practices within the meaning of the CFA, N.J.S.A. § 56:8-1, *et seq*.

143. Unlawful conduct under the CFA includes "deception, fraud, false pretense, false promise, misrepresentation."

144. As set forth above, Defendant committed deception, fraud, false pretenses, false promises, or misrepresentations about its data security. Defendant's representations were made with the intent to generate public good will and to induce consumers, such as Plaintiff and the other Subclass members, to reasonably rely on those representations and choose Defendant when making a decision about who to entrust their PII to.

145. Defendant's acts and practices as described herein deceived Plaintiff and the Subclass and were highly likely to deceive members of the consuming public. Plaintiff would not have entrusted her PII to Defendant had Plaintiff been aware that Defendant would unconscionably and unfairly place fail to safeguard her PII. Had Plaintiff and the other Subclass members entrusted their PII to a different bank, their PII would not have been exposed due to Defendant's reckless and intentional acts. Accordingly, Plaintiff and each member of the Subclass have suffered ascertainable loss as a direct result of Defendant's practices described above.

RELIEF REQUESTED

Plaintiff, individually and on behalf of the proposed Class, requests that the Court:

1. Certify this case as a class action on behalf of the Class defined above, appoint Plaintiff as class representative, and appoint the undersigned counsel as class counsel;

2. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and other Class Members;

3. Award restitution and damages to Plaintiff and Class Members in an amount to be determined at trial;

4. Award Plaintiff and Class Members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

5. Award Plaintiff and Class Members pre- and post-judgment interest, to the extent allowable; and

6. Award such other and further relief as equity and justice may require.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable of right.

Respectfully submitted,

/s/ Brian D. Flick
Brian D. Flick (OH #0081605)
Marc E. Dann (*pro hac vice* forthcoming)

DannLaw
P.O. Box 6031040
Cleveland, Ohio 44103
Phone: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

Javier Merino (*pro hac vice* forthcoming)
DANNLAW
372 Kinderkamack Road, Suite 5
Westwood, NJ 07675
Phone: 216-373-0539
Fax: 216-373-0536
jmerino@dannlaw.com

Terence R. Coates (*pro hac vice* forthcoming)
Zachary C. Schaengold (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
zschaengold@msdlegal.com

Counsel for Plaintiff, the Class, and Subclass

EXHIBIT A

Flagstar Bank

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

March 15, 2021

[redacted]

Notice of Data Breach

Dear [redacted]

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.

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.