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

PHILIP ANGUS, MARK WIEDDER, TANIA GARCIA, EDWARD BURDICK, RAY HARTER, DANIELLE MEIS, JONTHAN KELLEY, RYAN MARTIN, ARTHUR DORE, ANN KELLY, KEITH KELLY, RANDY MONIZ, and HOLLY RINGLING,

on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

FLAGSTAR BANK, N.A., f/k/a FLAGSTAR BANK, FSB, a Michigan-based federally chartered stock savings bank,

Defendant.

Case No.: 2:21-cv-10657-MFL-DRG

**FOURTH CONSOLIDATED CLASS ACTION COMPLAINT**

DEMAND FOR JURY TRIAL

## INTRODUCTION

**"You are a target, but don't be an easy one.** … You have data and information that is valuable to cyber criminals… Being proactive about cyber safety is the best way to protect yourself from potential harm."

*Protecting Your Identity*, FLAGSTAR.COM.

1. Flagstar is a publicly traded company organized and operated for the profit and financial benefit of its shareholders. It is the second largest mortgage

warehouse lender nationally, the seventh largest bank mortgage originator nationally, and the fifth largest sub-servicer of mortgage loans nationwide, serving over 1.4 million accounts with $382.2 billion in unpaid principal balances.

2. Flagstar's prospective, current, and former customers entrust Flagstar with vast troves of their confidential personal information. Flagstar profits from that personal information, which it collects and stores on computer hardware that it controls even after the customer relationship ends. Flagstar knows that it has a duty to safeguard the PII it collects from disclosure to third parties, is keenly aware that its customers' PII is a prime target for cyber criminals and has repeatedly acknowledged that the bank is at a high risk for cyberattacks.

3. Yet, for years leading up to the Data Breach, Flagstar used a near-obsolete file sharing platform from the early 2000's, licensed from its vendor Accellion, Inc. (the "FTA" platform), to share, and then indefinitely store, unencrypted loan applications, account applications, and other highly sensitive documents containing the Social Security numbers, financial account numbers, and other PII of over 1.4 million current and former customers and employees.

4. By January of 2021, the month Flagstar was breached, Flagstar knew that continued use of the FTA was highly dangerous for its customers' data—Accellion had advised Flagstar to discontinue use of, and had not permitted new customers to license, the outdated technology for nearly three years; the FTA had

not received regular security updates for over a year; the FTA had been running on an end-of-life, unsupported operating system for over a month; and, critically, the FTA had become the target of a concerted cyberattack nearly four weeks earlier. Flagstar knew each of these facts, yet not only failed to discontinue use of the highly vulnerable FTA, but failed to take any steps to protect the massive volumes of PII it was storing on it, like securely encrypting the data or clearing out unnecessary documents.

5. As a foreseeable consequence of Flagstar's reckless treatment of Plaintiffs' PII, cyber criminals infiltrated Flagstar's systems in January 2021 and exfiltrated documents stored on the FTA platform containing the sensitive personal information of over 1.4 million former and current Flagstar customers and employees.

## JURISDICTION AND VENUE

6. 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 Class Member is a citizen of a state different from Defendant, establishing minimal diversity.

7. 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.

8. 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.

## THE PARTIES

9. Plaintiffs are present or former customers or employees of Flagstar who entrusted Flagstar with their highly confidential and personally-identifiable information ("PII"),[1] which was then exfiltrated and compromised in the data breach announced by Flagstar on March 5, 2021 (the "Data Breach"). Plaintiffs bring this action on behalf of themselves and all those similarly situated both across the United States and within their State of residence. The following allegations are made upon

[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 C.F.R. § 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).

information and belief derived from, among other things, investigation of counsel, public sources, and the facts and circumstances as currently known. Because only Flagstar (and the cyber criminals) have knowledge of what information was compromised for each individual Plaintiff, Plaintiffs reserve their right to supplement their allegations with additional facts and injuries as they are discovered.

10. Defendant Flagstar Bank, N.A., f/k/a/ Flagstar Bank, FSB, is a Michigan-based federally chartered stock savings bank, headquartered at 5151 Corporate Drive, Troy, Michigan. New York Community Bancorp. Inc. is a Delaware corporation that is headquartered at 102 Duffy Avenue in Hicksville, New York. On December 1, 2022, New York Community Bancorp, Inc. merged with Flagstar Bancorp, Inc.[2] On September 23, 2023, NYCB unveiled a "refreshed logo and brand identity signaling the unification" of the companies "under the Flagstar name."[3] All of Plaintiffs' claims stated herein are asserted against Flagstar and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

---

[2] *Press Release: New York Community Bancorp, Inc. Completes Acquisition of Flagstar Bancorp, Inc.*, NEW YORK COMMUNITY BANCORP, INC., https://ir.mynycb.com/news-and-events/news-releases/press-release-details/2022/NEW-YORK-COMMUNITY-BANCORP-INC.-COMPLETES-ACQUISITION-OF-FLAGSTAR-BANCORP-INC/default.aspx (last visited May 9, 2024).

[3] *About Flagstar*, WWW.FLAGSTAR.COM, *available at* https://www.flagstar.com/about-flagstar.html (last visited May 9, 2024).

11. While its regional headquarters is in Troy, Michigan, Flagstar "has strong footholds in the Northeast and Midwest and exposure to high growth markets in the Southeast and West Coast."[4] Flagstar operates 419 branches nationwide, 100 private client banking teams, and a wholesale network of approximately 3,000 third-party originators.[5]

12. Flagstar's mortgage division was the seventh largest bank originator of residential mortgages for the 12-months ended December 31, 2023, and is the industry's fifth largest sub-servicer of mortgage loans nationwide, servicing 1.4 million accounts with $382.2 billion in unpaid principal balances as of December 31, 2023. Flagstar's parent company is the second largest mortgage warehouse lender nationally based on total commitments.[6] As of March 31, 2024, Flagstar manages $112.9 billion in assets, $83.3 billion of loans, deposits of $74.9 billion, and total stockholders' equity of $8.4 billion.[7]

[4] *About Flagstar*, WWW.FLAGSTAR.COM, *available at* https://www.flagstar.com/about-flagstar.html (last visited May 9, 2024).
[5] *Id.*
[6] Annual Report for 2023 on Form 10-K, NEW YORK COMMUNITY BANCORP, INC.
[7] *Id.*

## STATEMENT OF FACTS

### I. Flagstar Collects, Stores, and Profits from its Customers and Employees' PII.

13. To run its business, Flagstar collects, stores, shares, and profits from a treasure trove of personal information from its customers and employees, including Social Security numbers, email addresses, phone numbers, financial account information, credit scores, transaction histories, drivers' license and passport information, and more.[8] This highly sensitive PII is stored on centralized servers maintained by Flagstar. Flagstar collects this PII from all customers and maintains and profits from the PII regardless of whether a customer terminates their relationship with Flagstar; Flagstar maintains the PII of former customers for an indefinite period of time.

14. Flagstar's Privacy Policy is available on its website and provides customers with detailed promises regarding the treatment of their PII, including how Flagstar uses and shares customers' data for its own benefit and profit.[9] Flagstar explains that it collects customers' PII when customers "[o]pen an account or deposit money," "[p]ay [] bills or apply for a loan," or "[u]se [their] debit card."[10] Flagstar

---

[8] *Id.*
[9] *About Your Privacy*, WWW.FLAGSTAR.COM, https://www.flagstar.com/content/dam/flagstar/pdfs/ about-flagstar/PrivacyPolicy.pdf (last visited June 16, 2023).
[10] *Id.*

also collects customers' personal information from numerous third parties, including "[f]rom you," "[f]rom your devices when you interact with our websites, mobile applications and systems," "[f]rom you when you apply for and receive products and services," "[f]rom Flagstar employees when you interact with them and provide PI," "[f]rom brokers, correspondents, appraisers, legal counsel, government-sponsored entities, investors, prior servicers, credit bureaus and other public records," and "[f]rom beneficiaries, counterparties and other third parties related to a transaction."[11]

15. Flagstar profits from its customers' PII by using it for wide-ranging business and commercial purposes, including "[t]o market and our products and services."[12] Flagstar also profits from its customers' PII by sharing it with several categories of third parties, like insurance and credit card companies, for "joint marketing" purposes including "cross-context behavioral advertising," (e.g., targeting advertising) and "personalized ads."[13] Flagstar profits from its customers' PII even after the customer relationship ends: "When you are *no longer* our customer," Flagstar concedes, "we continue to share your information[.]"[14]

---

[11] *California Privacy Notice & Policy*, WWW.FLAGSTAR.COM, https://www.flagstar.com/legal-disclaimers/ccpa-privacy-notice.html (last visited June 16, 2023).
[12] *Id.*
[13] *Id.*
[14] *Id.* (emphasis in original).

16. After listing the ways Flagstar benefits from tracking and targeting its customers through collecting and maintaining their valuable PII, Flagstar's Privacy Policy pledges to them that their PII is secure, stating: "[t]o protect your personal information from unauthorized access and use, we use security measures that comply with federal law," and "[t]hese measures include computer safeguards and secured files and buildings."[15]

17. Along with its Privacy Policy, Flagstar maintains a "Fraud Information Center," on its website, and agrees and promises that "Flagstar is committed to your financial security,"[16] acknowledging that "[r]apid advances in technology and creative criminal minds [that] make fraud a potentially serious threat on a variety of fronts."[17] In recognition of the highly sensitive nature of the information that it obtains from its customers, as well as the damages that can be inflicted on consumers if this information is in the hands of identity thieves, Flagstar commits to its clients that "[p]rotecting your finances is a top priority," and warns them that "[s]ecuring your financial information is essential to protecting your finances."[18]

---

[15] *Id.*
[16] *Fraud Information Center*, WWW.FLAGSTAR.COM, https://www.flagstar.com/fraud-information-center.html (last visited June 16, 2023).
[17] *Id.*
[18] *Preventing Fraud*, WWW.FLAGSTAR.COM, https://www.flagstar.com/fraud-information-center/preventing-fraud.html (last visited June 16, 2023).

18. "That's why," Flagstar represents, "we closely monitor all types of white-collar crime, including identity theft and the rapidly growing area of mortgage fraud."[19] Flagstar further promises its customers that they have "firewalls and prevention systems that stop unauthorized access to our network computers, plus secure network protocols that ensure connections between our offices, partners, and customers."[20] Flagstar's webpage dedicated to "Data Security and Customer Privacy," reiterates that Flagstar has "built processes to identify cybersecurity threats and ensure our data and customer privacy are well-protected."[21]

## II. Flagstar's Use of the Legacy FTA Platform.

19. Accellion, Inc. ("Accellion") is a cloud solutions company that developed, marketed, and sold a file sharing transfer software product called File Transfer Appliance ("FTA") platform starting in the early 2000s. The purpose of the FTA was to facilitate file sharing that exceeded limits imposed on the size of email attachments. Instead of transferring documents by email, the intended recipient would receive a link to files on the FTA, which could then be viewed or downloaded.

20. Sometime before 2016, Flagstar licensed the FTA platform from Accellion to facilitate large file transfers. FTA customers could host the software on

---

[19] *Id.*
[20] *Id.*
[21] *Data Security and Customer Privacy*, WWW.FLAGSTAR.COM, https://www.flagstar.com/esg/governance/data-security-and-customer-privacy.html (last visited May 12, 2024).

the customers' own systems. FTA customers were responsible for managing, maintaining, and updating their instances of the FTA software.

21. Flagstar implemented the FTA platform within its network and, until it was breached in January 2021, used it to store, stage, send, and receive documents containing the PII of its present and former customers and employees, including mortgage approvals, applications, and other types of sensitive document transfers containing Plaintiffs' most valuable information. Flagstar did so for years even though Flagstar knew or should have known that its implementation and use of the FTA platform put its customers' and employees' PII at an unjustifiably high risk.

22. The Financial Services sector is one of the most targeted sectors by cyber criminals,[22] and for nearly a decade, Flagstar has known that the cybersecurity of Flagstar and its vendors in relation to customers' PII is one of the most significant risks faced by the company.[23]

23. In its 2012 annual report, Flagstar acknowledged that because it conducts business "over the Internet" and "outsource[s] critical functions to third

[22] *For Financial Institutions, Cyberthreats Loom Large*, FORBES, https://www.forbes.com/sites/forbesfinancecouncil/2022/03/09/for-financial-institutions-cyberthreats-loom-large/?sh=69dd96d82ddb (last accessed June 16, 2023).

[23] *Investor Bulletin: How to Read a 10-K*, SEC, *available at* https://www.sec.gov/files/reada10k.pdf (last visited May 7, 2024) (explaining that items listed in 1A "Risk Factors" of a company's 10-K report reflect the "most significant risks" that apply to the company).

parties," its operations "depend on our ability…to protect computer system and network infrastructure[.]"[24] In the report, Flagstar cited the cybersecurity risk of using "third-party service providers" due to "advances in computer capabilities," and warned that any breach of its vendors would pose a threat to customer data.[25] Flagstar further acknowledged the "rapidly expanding and evolving cybersecurity threats that exist today[,]" and noted that "techniques used [by cyber criminals] tend to change frequently" and attacks "can originate from a wide array of sources[.]" "As cybersecurity threats continue to evolve," Flagstar conceded "we may be required to expend additional resources to continue to modify or refine our protective measures against these threats."[26]

24. In its 2015 annual report, Flagstar reiterated that "[d]ata breaches are of a particular concern" for Flagstar because it receives, transmits, and stores "a large volume of personally identifiable information and other user data."[27]

---

[24] Form 10-K Annual Report for 2012 ("2012 Report"), FLAGSTAR BANK, *available at* https://www.sec.gov/Archives/edgar/data/1033012/000103301213000018/fbc-20121231x10k.htm.
[25] *Id.*
[26] *Id.*
[27] Form 10-K Annual Report for 2015 ("2015 Report"), FLAGSTAR BANK, *available at* https://www.sec.gov/Archives/edgar/data/1033012/000103301216000110/fbc-20151231xform10k.htm.

25. Flagstar knowingly failed to protect its customers' PII against the rapidly expanding and evolving cybersecurity threats.

26. In January 2014, Accellion launched the FTA's successor product, Kiteworks, a more secure file transfer software that was constructed on an "entirely different code base," than the FTA, "using state-of-the-art security architecture, and a segregated, secure devops process."[28] Archived webpages from Accellion's website demonstrate that Accellion publicly identified key security features in Kiteworks that were not available for the FTA platform; they also suggest that, by the time Accellion released Kiteworks in 2014, Accellion was no longer actively marketing the FTA platform. If Flagstar licensed the FTA after Kiteworks was launched, this suggests that Flagstar was likely pitched the Kiteworks product and chose to knowingly license a legacy and sub-standard file transfer product with known security vulnerabilities.

27. By the end of 2016, Accellion stopped licensing the FTA product to new customers altogether. Although Accellion permitted existing customers (like Flagstar) to extend their licenses for the FTA, Accellion advised them to transition to Kiteworks.[29]

---

[28] *Press Release: Accellion Provides Update to FTA Security Incident*, KITEWORKS.COM (Feb. 22, 2021).

[29] *See, e.g., Accellion's Motion to Dismiss*, Case No. 5:21-cv-01155-EJD, Dkt. 174 at 11 (N. D. Cal. July 31, 2023) ("Some Accellion customers, such as Flagstar Bank… opted to use a legacy Accellion product to transfer and store data…. They

28. For at least two years before the Data Breach, Accellion dedicated a portion of its website to encouraging customers on the legacy FTA platform to migrate to Kiteworks, publicly comparing specific security features present in the "new platform" (Kiteworks) that were not available in the FTA, including encryption for data "at rest."[30]

29. Instead of transitioning to Kiteworks or another more secure software, Flagstar chose to continue to license the FTA even though Flagstar knew or should have known about specific security deficiencies in the FTA platform, as well as its status as a vulnerable "legacy" product that was operating on 16-year-old code and was no longer offered in the marketplace.

30. For the next four years, from 2016-2020, thirty-six serious security vulnerabilities for the legacy FTA platform were publicly disclosed, including the same type of vulnerability repeatedly used to compromise the product in December

---

did so notwithstanding that Accellion had advised them to migrate to its newer, more modern file-transfer product."); *Press Release: Accellion Provides Update to Recent FTA Security Incident*, KITEWORKS.COM (Feb. 1, 2021), *available at* https://www.kiteworks.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last accessed May 8, 2024); *see Press Release: Accellion Announces End of Life (EOL) for its Legacy FTA Product*, KITEWORKS.COM (Feb. 25, 2021) ("For the past three years, Accellion has been attempting to move existing FTA customers over to our more modern and more secure platform").

[30] *See Accellion FTA Overview*, ACCELLION.COM (version as of Dec. 30, 2019), *available at* https://web.archive.org/web/20191230154137/https://www.accellion.com/products/fta/ (last accessed May 12, 2024).

2020, a SQL vulnerability. These vulnerabilities were published on the internet on free, government-sponsored sources that catalog publicly known software or firmware vulnerabilities.[31] These vulnerabilities were also circulated via notices and alerts from industry groups like the Financial Services Information Sharing and Analysis Center's ("FS-ISAC"). Flagstar was responsible for reading the alerts on vendors it deployed within its environment and taking appropriate action. Flagstar continued to license the FTA despite the fact that it knew or should have known of persistent, critical vulnerabilities that continued to be uncovered.

31. Flagstar also continued to license the FTA as cybersecurity risks continued to rise for the financial services sector. In 2016, the Homeland Security Advisor Council (HSAC) warned that the Financial Services sector faced rapidly growing cyber threats.[32] The chair of the Securities and Exchange Commission (SEC) warned that cybersecurity was the biggest risk to the financial system.[33] The following year, in 2017, the National Infrastructure Advisory Council (NIAC) issued a report titled "Addressing Urgent Cyber Threats to Critical Infrastructure," advising

[31] CVE Database, THE MITRE CORPORATION, *available at* https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Accellion (last accessed May 7, 2024).
[32] HSAC, *Final Report of the Cybersecurity Subcommittee: Part I-Incident Response*, 2016.
[33] Lisa Lambert and Suzanne Barlyn, *SEC says cyber security biggest risk to financial system*, REUTERS (May 18, 2016), *available at* https://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4/ (last accessed May 8, 2024).

that "[t]oday's cyber attacks are increasingly dangerous and targeted, designed by advanced actors to damage or disrupt critical U.S. infrastructure that deliver vital services—particularly…financial services."[34] According to a 2019 Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report, of the 1,473 recorded data breaches, 108 of them were in the financial services sector, responsible for 62% of the 164 million sensitive records exposed in 2019.[35]

32. In its annual reports for 2017, 2018, 2019, and 2020, Flagstar repeatedly acknowledged that "[c]ybersecurity risks for banking institutions have increased significantly in recent years due to new technologies, the reliance on technology to conduct financial transactions and the increased sophistication of organized crime and hackers."[36] Flagstar explained that "[c]ybersecurity related attacks are attempted

[34] *Securing Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure*, THE PRESIDENT'S NATIONAL INFRASTRUCTURE ADVISORY COUNCIL (Aug. 2017), *available at* https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf (last accessed May 8, 2024).

[35] *2019 End-of-Year Data Breach Report*, IDENTITY THEFT RESOURCE CENTER, https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited June 26, 2023); *62% of breached data came from financial services in 2019*, CIO DIVE, *available at* https://www.ciodive.com/news/62-of-breached-data-came-from-financial-services-in-2019/569592/ (last visited June 16, 2023); *Bitglass' 2019 Financial Breach Report*, BITGLASS.

[36] Form 10-K Annual Report for 2017 ("2017 Report"), FLAGSTAR BANK, *available at* https://www.sec.gov/Archives/edgar/data/1033012/000103301218000025/fbc-

on an ongoing basis which pose a risk…[to] customers' personally identifiable information[.]"[37]

33. In 2019, Flagstar acknowledged its responsibility to manage third-party software to keep Plaintiffs' PII secure. Admitting that "[i]ncreased risk could occur based on poor planning, oversight, [or] control" of third-party vendors, Flagstar explained that it had "implemented a vendor management program to actively manage the risks associated with the use of third-party service providers[.]"[38] Flagstar explained that its "Vendor Management" department "provides oversight related to the overall risk management process associated with third-party relationships."[39] Flagstar was explicit that Flagstar management was "accountable for the review and evaluation of all new and existing third-party relationships and is responsible for ensuring that adequate controls are in place to protect us and our

---

20171231xform10k.htm; Form 10-K Annual Report for 2018 ("2018 Report"), FLAGSTAR BANK, *available at* https://www.sec.gov/Archives/edgar/data/1033012/000103301219000033/fbc-20181231xform10k.htm; Form 10-K Annual Report for 2019 ("2019 Report"), FLAGSTAR BANK, *available at* https://www.sec.gov/ix?doc=/Archives/edgar/data/0001033012/000103301220000017/fbc-20191231xform10k.htm; Form 10-K Annual Report for 2020 ("2020 Report"), FLAGSTAR BANK, *available at* https://www.sec.gov/ix?doc=/Archives/edgar/data/0001033012/000103301221000037/fbc-20201231.htm.

[37] 2020 Report (emphasis added).

[38] 2019 Report.

[39] *Id.*

customers from the risks associated with vendor relationships."[40] According to Flagstar, "[t]he risks associated with the vendor activity are not passed to the third-party but remain our responsibility."[41]

34. In February 2019, Accellion released its last security update for the FTA platform until the cyberattacks began in December 2020.[42] By early 2020, most of the hold-out FTA customers had migrated from FTA to Kiteworks.[43] Indeed, Accellion had continued to advise the remaining FTA customers to switch to Kiteworks by making it cheaper for FTA customers to switch than to stay on FTA and offering technical support for the transition. Archived versions of Accellion's website show that at least as of October 2018, Accellion was providing customers "free installation and migration services" for customers to transition from FTA to Kiteworks.[44]

35. In 2020, Flagstar faced even more heightened cybersecurity risks due to the COVID-19 pandemic and its institution of a "work-from-home" policy. In its

---

[40] *Id.*
[41] *Id.*
[42] In contrast, Accellion represented that the Kiteworks software "is updated on an agile quarterly release cycle[.]" *Accellion FTA Attack Customer FAQs*, ACCELLION (March 1, 2021), *available at* https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-customer-faqs.pdf (last accessed May 8, 2024).
[43] *Id.*
[44] *Accellion Home Page*, ACCELLION.COM (as of Oct. 2018), *available at* https://web.archive.org/web/20181031150257/https://www.accellion.com/ (last accessed May 13, 2024) (selected "Platform" dropdown).

2020 annual report, Flagstar acknowledged that COVID-19 and related work-from-home policies "expos[ed] us to increased cybersecurity risk[,]" and admitted that Flagstar had "observed an increase in attempted malicious activity from third parties directed at the Bank…such as attempts to obtain personally identifiable information."[45] Other organizations facing this increased cybersecurity risk from the "shift to remote work during the pandemic" opted to "retire legacy file transfer technology[.]"[46]

36. In the months before the Data Breach, the threats against financial firms continued to rise. On July 10, 2020, the SEC issued a warning about a rise in ransomware attacks on U.S. financial firms.[47] On October 14, 2020, Mandiant warned that FIN11 (one of the cyber criminals involved in the Data Breach) had "successfully monetized" cyberattacks and that it "has deployed CLOP ransomware and threatened to publish exfiltrated data to pressure victims into paying ransom demands."[48] At a press conference on December 8, 2020, FBI Director Christopher

---

[45] *Id.*

[46] Mathew Schwartz, *Accellion Holdouts Get Legacy File Transfer Appliance Blues*, BANK INFO SECURITY (Mar. 30, 2021), *available at* https://www.bankinfosecurity.com/blogs/accellion-holdouts-get-legacy-file-transfer-appliance-blues-p-3009 (last accessed May 9, 2024).

[47] *Cybersecurity: Ransomware Alert*, SEC (July 10, 2020), *available at* https://www.sec.gov/ocie/announcement/risk-alert-ransomware (last accessed May 8, 2024).

[48] *FIN11: Widespread Email Campaigns as Precursor for Ransomware and Data Theft*, MANDIANT (Oct. 14, 2020), *available at*

Wray warned banks to be aware of "cyber criminals targeting the vulnerabilities in third-party services" as a way into financial institution data.[49]

37. In Flagstar's 2020 annual report, Flagstar admitted that both Flagstar and its "third-party providers are regularly the subject of attempted attacks and the ability of the attackers continues to grow in sophistication."[50] Flagstar reiterated that "[w]e, and our third-party providers, have been in the past and may in the future be subject to cybersecurity attacks."[51] In 2021, Steven Silberstein, CEO of the Financial Services Information Sharing and Analysis Center, confirmed that they were "seeing a clear trend of attacks on third-party suppliers, especially software vendors, to the financial sector[.]"[52]

38. Then, on November 30, 2020, the FTA's operating system, CentOS 6, reached its end-of-life (EOL). CentOS 6's end-of-life date had been publicly announced more than a year earlier. According to Security Week, Accellion had warned FTA customers six months earlier that CentOS would be EOL as of

---

https://www.mandiant.com/resources/blog/fin11-email-campaigns-precursor-for-ransomware-data-theft (last accessed May 8, 2024).

[49] *See Timeline of Cyber Incidents Involving Financial Institutions: FBI Warns of Third-Party Service Attacks*, CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE, *available at* https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline (last accessed May 8, 2024).

[50] *Id.*

[51] *Id.* (emphasis added).

[52] Penny Crosman, *Flagstar's data breach, and what we can learn from it*, AMERICAN BANKER (Mar. 15, 2021).

November 30, 2020.[53] This change rendered use of the FTA highly dangerous.[54] For the year leading up to November 30, 2020, Flagstar knew or should have known that the already-vulnerable FTA was going to be operating on an unsupported and highly-vulnerable system as of November 30, 2020, and should have at least migrated to a more secure platform during that time frame; once November 30, 2020 arrived, Flagstar should have quit use of the platform immediately.

39. Despite these well-known and mounting risks to Plaintiffs' PII, Flagstar continued to use the FTA platform without instituting any meaningful protections for the customer information stored therein, making its customers' PII an easy target.

## III. The Data Breach.

40. By December 2020, the FTA product was an almost 20-year-old

[53] Ionut Arghire, *Accellion to Retire File Transfer Service Targeted in Attacks*, Security Week (Feb. 15, 2021), *available at* https://www.securityweek.com/accellion-retire-file-transfer-service-targeted-attacks/ (last accessed May 9, 2024).

[54] *See CentOS-6 Reaching End of Life in November 2020*, HOST DIME (Dec. 17, 2019), *available at* https://www.hostdime.com/blog/centos-6-end-of-life/ (last accessed May 10, 2024) ("CentOS-6 will reach End of Life on November 30, 2020. End of Life means a product is no longer supported. CentOS will no longer provide security updates or fix bugs."); *CentOS 6 EOL*, SYSBEE (Nov. 24, 2020), *available at* https://www.sysbee.net/blog/centos-6-eol/ (last accessed May 10, 2024) ("CentOS 6 will reach EOL on 30th November 2020. In practice, this means that any new bug or vulnerability found on CentOS won't be addressed. EOL technologies won't receive any security patches from the providers, meaning they are left vulnerable to security breaches.").

product nearing end-of-life, operating on an end-of-life operating system.[55] Of Accellion's thousands of customers, Flagstar was one of only approximately 300 hold-out FTA customers that had failed to transition to Accellion's new platform.

41. On December 16, 2020, cyber criminals associated with FIN11, a financially motivated criminal group, began "a concerted cyberattack on the Accellion FTA product that continued into January 2021."[56]

42. That day, an Accellion customer received an alert from the FTA product's built-in anomaly detector signaling that unauthorized third parties had exploited the FTA. The customer notified Accellion, and over the next three days, Accellion determined that threat actors used a traditional SQL injection methodology to gain access and then extract personal information.[57]

43. The cyberattack was "specific to the FTA software" and was "specifically engineered to help identify and exfiltrate files stored in a customer's

---

[55] *Press Release: Accellion Provides Update to Recent FTA Security Incident*, KITEWORKS.COM (Feb. 1, 2021), *available at* https://www.kiteworks.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last accessed May 8, 2024).

[56] *Press Release: Bad Practices*, CYBERSECURITY INFRASTRUCTURE & SECURITY AGENCY (Feb. 1, 2021), *available at* https://www.cisa.gov/news-events/news/bad-practices-0 (last accessed May 8, 2024).

[57] Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC (Feb. 24, 2021), *available at* https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/ (last accessed May 8, 2024).

FTA system."[58] According to cybersecurity firm Coveware, "data theft from the appliance was the sole target of [the criminals'] campaign from the outset."[59]

44. On December 20, 2020, Accellion released a patch to all FTA customers, including Flagstar, stating that the matter was "critical and time sensitive," and "strongly encouraging customers" to update their systems "as soon as possible."[60]

45. On December 23, 2020, Accellion notified FTA customers, including Flagstar, that the FTA was being attacked.[61] Flagstar knew the FTA was being attacked by cyber criminals as of December 23, 2020, yet continued to not only use the FTA platform, but continued to store the PII of over 1.4 million consumers on the FTA platform for nearly four weeks, without notifying its customers or taking any action to protect their data.

---

[58] *Accellion FTA Attack Customer FAQs*, ACCELLION (March 1, 2021), *available at* https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-customer-faqs.pdf (last accessed May 8, 2024).

[59] Quarterly Report, *Ransomware Attack Vectors Shift as New Software Vulnerability Exploits Abound*, COVEWARE (Apr. 26, 2021), *available at* https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound (last accessed May 8, 2024).

[60] *Accellion FTA Attack Customer FAQs*, ACCELLION (March 1, 2021), *available at* https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-customer-faqs.pdf (last accessed May 8, 2024).

[61] *Press Release: Accellion Provides Update to Recent FTA Security Incident*, KITEWORKS.COM (Feb. 1, 2021), *available at* https://www.kiteworks.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last accessed May 8, 2024).

46. On January 4, 2021, Accellion sent a reminder email to FTA customers to update their systems.[62]

47. On January 12, 2021, Accellion issued a Press Release publicly announcing the "FTA Security Incident."[63] In the release, Accellion emphasized that the FTA "is a 20 year old product," and that its "flagship enterprise content firewall platform, kiteworks, was not involved" in the attacks.[64]

48. On January 20, 2021, cyber criminals launched their second attack on FTA platform customers. Accellion learned of the second attack on January 22, 2021, after multiple customers complained of anomalous behavior.[65] That day, Accellion issued an urgent security alert to FTA customers, including Flagstar, advising them to shut down their FTA systems immediately.[66] Flagstar has suggested

[62] *Accellion FTA Attack Customer FAQs*, ACCELLION (March 1, 2021), *available at* https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-customer-faqs.pdf (last accessed May 8, 2024).
[63] *Press Release: Accellion Responds to Recent FTA Security Incident*, ACCELLION (Jan. 12, 2021), *available at* https://www.kiteworks.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/ (last accessed May 8, 2024).
[64] *Id.*
[65] *Accellion FTA Attack Customer FAQs*, ACCELLION (March 1, 2021), *available at* https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-customer-faqs.pdf (last accessed May 8, 2024).
[66] *Id.*

that it did not learn of unusual behavior on the platform until Accellion sent the security alert.[67]

49. GuidePoint Security explained that the cyber criminals uploaded a "web shell" to the targeted FTA servers which leveraged a SQL injection vulnerability to install itself into the FTA server, providing the criminals with the ability to download files stored there. The web shell was designed "specifically to be uploaded to an Accellion FTA server" which was "a similar scenario [that] ha[d] been observed with the [FTA] platform in 2016[.]"[68] Specifically, the cyber criminals attacked the platform using:

a. SQL Injection: a vulnerability that is present when the developer fails to validate the various types of input allowed to query the information contained in its database. This vulnerability has been known and methods to detect and prevent have been documented since 1997 and is present in most security training and nearly all security testing tools and scanners. The Accellion FTA application had over two dozen high

[67] *Accellion Incident Information Center*, FLAGSTAR.COM (as of March 24, 2021), *available at* https://web.archive.org/web/20210324170649/https://www.flagstar.com/customer-support/accellion-information-center.html (last accessed May 8, 2024) ("Accellion…informed Flagstar on January 22, 2021, that the platform had a vulnerability that was exploited by an unauthorized party").

[68] Drew Schmitt, *Accellion FTA Targeted by Web Shell*, GUIDEPOINT SECURITY (Jan. 28, 2021), *available at* https://www.guidepointsecurity.com/blog/accellion-fta-targeted-by-file-downloading-web-shell/ (last accessed May 8, 2024).

severity SQL injection vulnerabilities between 2016 and 2021, all of which were publicly listed.

b. OS Command Execution: a vulnerability that allows an unauthorized user to execute native commands in the system using tools and services already present in the system. This is also called ACE (Arbitrary code execution). It is prevented through monitoring, logging, and alerting. This vulnerability has been known and is able to be tested and prevented for several decades.

c. Server Side Request Forgery: an attack vector that requires several other vulnerabilities to be present, including lack of network segmentation of the network and vulnerability to malicious web shells.

50. Once cyber criminals gained access to the FTA platform, they exfiltrated a massive number of unencrypted documents from Flagstar's system reflecting the PII of over 1.4 million people.

51. According to Flagstar, it was not until two days later, on January 24, 2021, that Flagstar determined that cyber criminals were able to access and exfiltrate sensitive documents and data from the FTA platform. While Flagstar has publicly stated that it "permanently discontinued use" of the FTA platform "[a]fter Accellion informed us of the incident," Flagstar has not disclosed exactly when Flagstar did so, nor has it disclosed when the cyber criminals exfiltrated data.

52. Soon after the cyber criminals exfiltrated data from the FTA platform, Flagstar received a ransom note from criminals associated with the CLOP ransomware gang threatening to release stolen data online if a ransom payment was not made.[69]

53. Then, on March 8, 2021, the CLOP ransomware gang "doxed" several Flagstar employees by posting their social security numbers and home addresses on CLOP's dark web "leak" site in an attempt to extort money from the bank.[70] The site displayed a table that included the names, social security numbers, and home addresses of eighteen alleged employees of Flagstar, and the hackers also posted other documents that included private personal information.[71] The post was joined by the statement: "Want to delete a page or buy data? Write to the email indicated on the home page. We have a lot of private personal information including the SSN, addresses, and phone numbers etc… of your clients and employees."[72] CLOP then

---

[69] Mandiant attributed the cyberattacks to both FIN11, believed to be responsible for compromising the system, and the CLOP ransomware gang, believed to be responsible for engaging in extortion activity with some of the compromised customers, including Flagstar.

[70] *Ransomware Gang Fully Doxes Bank Employees in Extortion Attempt*, VICE.COM (Mar. 8, 2021), *available at* https://www.vice.com/en/article/3an9vn/ransomware-gang-fully-doxes-bank-employees-in-extortion-attempt (last accessed May 8, 2024).

[71] *Id.*

[72] *Id.*

emailed reporters to advertise the extortion attempt, explaining that they published the data hoping to convince Flagstar to pay them to stop leaking its internal data.[73]

54. According to Vice, a "source familiar with the bank" said that Flagstar engaged in ransom negotiations with CLOP in an attempt "to buy time…before the threat actor started leaking data."[74]

55. Soon after its initial dark web post, CLOP posted over 80 gigabytes of information stolen from Flagstar during the Data Breach on the dark web. These downloadable files remain available on the dark web as of May 1, 2024, and have been copied from CLOP's original post to a "mirror" dark web site, ensuring their permanent status on the dark web.

56. After the data breach, Flagstar acknowledged that "those responsible for this incident are in some cases contacting Flagstar customers by e-mail and by telephone[,]" stating, "[t]hese are communications from unauthorized individuals responsible for the Accellion incident, and you should not respond to them. If you receive a suspicious message, please do not open attachments or click on links. **Should you receive any engagement from anyone indicating they are in possession of your information, please reach out to us…immediately.**"

[73] *Id.*
[74] *Id.*

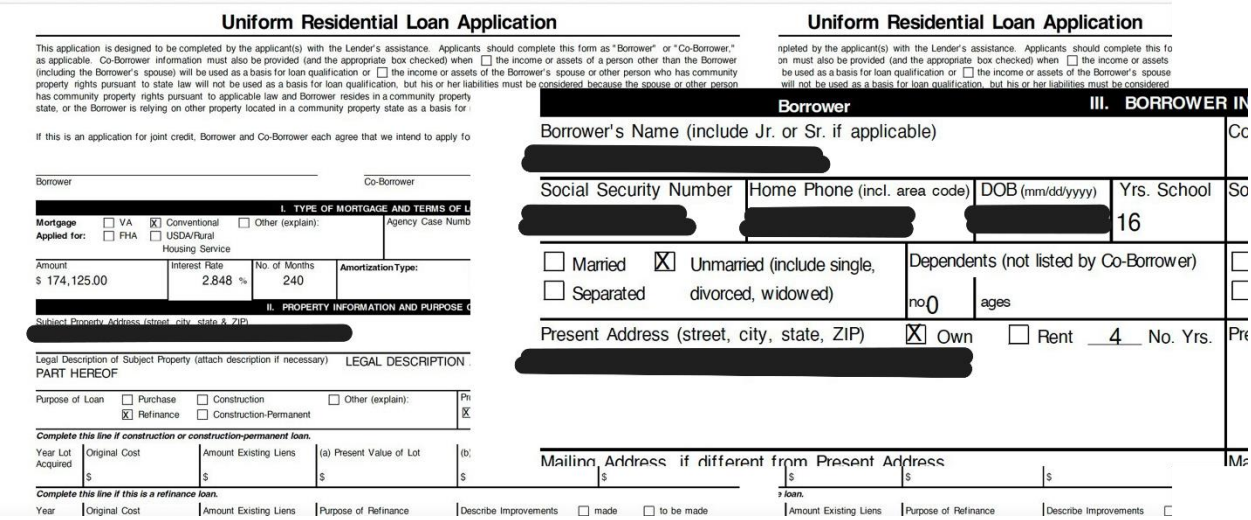
57. The information posted on the dark web is not simply a collection of isolated data points. Instead, the cyber criminals posted folders, cataloged by Flagstar employee's or customer's email addresses, which contain thousands of documents, including (1) mortgage applications (2) account applications; (3) collection calls; (4) internal spreadsheets, and a (5) wide variety of other information related to loan customers, banking customers, and employees, including:

a. Environmental site assessments (vacant land).
b. Customer bankruptcy documents.
c. Auto Cad floor plans of various buildings.
d. Bank inspection pictures including internal security features.
e. Spreadsheets with loan numbers, names and amount of loan.
f. Recorded mortgages.
g. W-9's.
h. Spreadsheets with name, address, SSN, DOB, loan numbers, and credit scores.
i. Payment letter to borrowers, including one that is 862 pages that has full tax returns, mortgage loan documents, domestic couple declarations, dependent information, bank statements with cancelled checks and other various documents used for loan applications.
j. Worker Health Benefits spreadsheets with dependent information.
k. Employee Master Data spreadsheet that includes all PII as well as salary amounts.
l. Business Auto Payment Forms with Tax ID and Account numbers.
m. Business checking statements with cancelled checks.
n. Disclosures regarding legal representation for closings.
o. Uniform Residential Loan Applications.
p. "The library" – all internal policies and procedures for Flagstar.
q. Customer Account Activity Statements.
r. Phone calls between hardship department and customers where full PII and contact information is given to Flagstar employee by the customer to verify the account.
s. Subpoenas from Office of Inspector General/Social Security Administration for banking information.
t. Loan comments – notes from calls with customers, contains some PII –

name, address, loan number, amount due, issue customer is having, etc.

58. Examples of information posted to the dark web include the following (which are not redacted on the dark web but are redacted here to preserve class members' privacy):

a. **Loan Application**



Uniform Residential Loan Application

This application is designed to be completed by the applicant(s) with the Lender's assistance. Applicants should complete this form as "Borrower" or "Co-Borrower," as applicable. Co-Borrower information must also be provided (and the appropriate box checked) when ☐ the income or assets of a person other than the Borrower (including the Borrower's spouse) will be used as a basis for loan qualification or ☐ the income or assets of the Borrower's spouse or other person who has community property rights pursuant to state law will not be used as a basis for loan qualification, but his or her liabilities must be considered because the spouse or other person has community property rights pursuant to applicable law and Borrower resides in a community property state, or the Borrower is relying on other property located in a community property state as a basis for

If this is an application for joint credit, Borrower and Co-Borrower each agree that we intend to apply fo

Borrower | Co-Borrower

I. TYPE OF MORTGAGE AND TERMS OF L

Mortgage Applied for: ☐ VA ☐ FHA ☒ Conventional ☐ USDA/Rural Housing Service ☐ Other (explain): | Agency Case Numb

| Amount | Interest Rate | No. of Months | Amortization Type: |
|---|---|---|---|
| $ 174,125.00 | 2.848 % | 240 | |

II. PROPERTY INFORMATION AND PURPOSE

Subject Property Address (street, city, state & ZIP) [redacted]

Legal Description of Subject Property (attach description if necessary) LEGAL DESCRIPTION PART HEREOF

Purpose of Loan ☐ Purchase ☐ Construction ☐ Other (explain): ☒ Refinance ☐ Construction-Permanent

*Complete this line if construction or construction-permanent loan.*

| Year Lot Acquired | Original Cost | Amount Existing Liens | (a) Present Value of Lot | (b) |
|---|---|---|---|---|
| | $ | $ | $ | $ |

*Complete this line if this is a refinance loan.*

Year | Original Cost | Amount Existing Liens | Purpose of Refinance | Describe Improvements ☐ made ☐ to be made

Uniform Residential Loan Application

npleted by the applicant(s) with the Lender's assistance. Applicants should complete this fo on must also be provided (and the appropriate box checked) when ☐ the income or assets be used as a basis for loan qualification or ☐ the income or assets of the Borrower's spouse will not be used as a basis for loan qualification, but his or her liabilities must be considered

Borrower III. BORROWER IN

Borrower's Name (include Jr. or Sr. if applicable) [redacted] Co

| Social Security Number | Home Phone (incl. area code) | DOB (mm/dd/yyyy) | Yrs. School | So |
|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | 16 | |

☐ Married ☒ Unmarried (include single, divorced, widowed) ☐ Separated

Dependents (not listed by Co-Borrower) no 0 ages

Present Address (street, city, state, ZIP) [redacted] ☒ Own ☐ Rent 4 No. Yrs. Pre

Mailing Address, if different from Present Address Ma

$ | $ | $

loan.

Amount Existing Liens | Purpose of Refinance | Describe Improvements

b. **Authorization for Release of Social Security Number**

Form **SSA-89** (02-2018)
Discontinue Previous Editions
Social Security Administration

Page 1 of 2
OMB No. 0960-0760

**Authorization for the Social Security Administration (SSA)**
**To Release Social Security Number (SSN) Verification**

| Printed Name: | Date of Birth: | Social Security Number: |
|---|---|---|
| [redacted] | [redacted] | [redacted] |

I want this information released because I am conducting the following business transaction:
Mortgage Application

Reason(s) for using CBSV: (Please select all that apply)
- [X] Mortgage Service
- [ ] Banking Service
- [ ] Background Check
- [ ] License Requirement
- [X] Credit Check
- [ ] Other

with the following company ("the Company"):

Company Name: _____

Company Address: _____

I authorize the Social Security Administration to verify my name and SSN to the Company and/or the Company's Agent, if applicable, for the purpose I identified.

The name and address of the Company's Agent is:
TALX Corporation
11432 Lackland Road, St. Louis, MO 63146

I am the individual to whom the Social Security number was issued or the parent or legal guardian of a minor, or the legal guardian of a legally incompetent adult. I declare and affirm under the penalty of perjury that the information contained

## c. Request for Transcript of Tax Return

Form **4506-T**
(March 2019)
Department of the Treasury
Internal Revenue Service

**Request for Transcript of Tax Return**

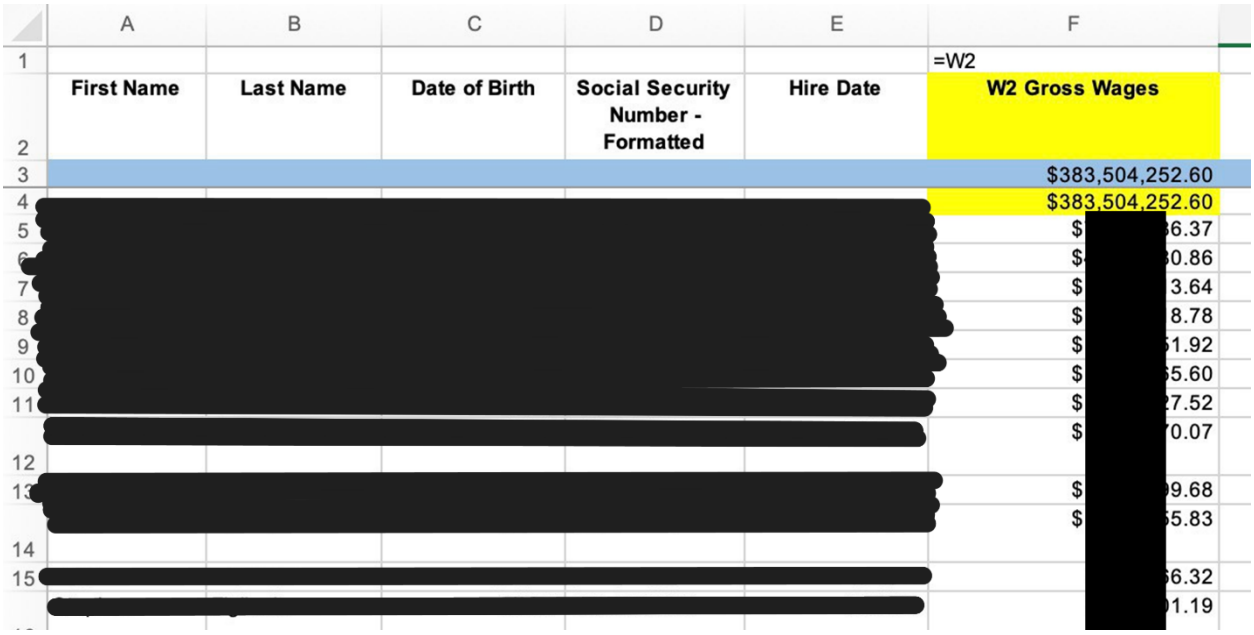
► **Do not sign this form unless all applicable lines have been completed.**
► **Request may be rejected if the form is incomplete or illegible.**
► **For more information about Form 4506-T, visit *www.irs.gov/form4506t.***

OMB No. 1545-1872
Loan Number: [redacted]

**Tip.** Use Form 4506-T to order a transcript or other return information free of charge. See the product list below. You can quickly request transcripts by using our automated self-help service tools. Please visit us at IRS.gov and click on "Get a Tax Transcript..." under "Tools" or call 1-800-908-9946. If you need a copy of your return, use **Form 4506, Request for Copy of Tax Return.** There is a fee to get a copy of your return.

| | | | |
|---|---|---|---|
| 1a | Name shown on tax return. If a joint return, enter the name shown first. [redacted] | 1b | **First social security number on tax return, individual taxpayer identification number, or employer identification number (see instructions)** [redacted] |
| 2a | If a joint return, enter spouse's name shown on tax return. | 2b | **Second social security number or individual taxpayer identification number if joint tax return** |
| 3 | Current name, address (including apt., room, or suite no.), city, state, and ZIP code (see instructions) [redacted] | | |
| 4 | Previous address shown on the last return filed if different from line 3 (see instructions) | | |
| 5a | If the transcript or tax information is to be mailed to a third party (such as a mortgage company), enter the third party's name, address, and telephone number. TALX Corporation, a provider of Equifax Verification Services 11432 Lackland Road, Saint Louis, MO 63146 | | |
| 5b | Customer file number (if applicable) (see instructions) | | |

## d. List of Flagstar Employee Information



| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | | | | | | =W2 |
| 2 | First Name | Last Name | Date of Birth | Social Security Number - Formatted | Hire Date | W2 Gross Wages |
| 3 | | | | | | $383,504,252.60 |
| 4 | [redacted] | | | | | $383,504,252.60 |
| 5 | | | | | | $ [redacted]6.37 |
| 6 | | | | | | $ [redacted]0.86 |
| 7 | | | | | | $ [redacted]3.64 |
| 8 | | | | | | $ [redacted]8.78 |
| 9 | | | | | | $ [redacted]1.92 |
| 10 | | | | | | $ [redacted]5.60 |
| 11 | | | | | | $ [redacted]7.52 |
| 12 | | | | | | $ [redacted]0.07 |
| 13 | | | | | | $ [redacted]9.68 |
| 14 | | | | | | $ [redacted]5.83 |
| 15 | | | | | | [redacted]6.32 |
| | | | | | | [redacted]1.19 |

59. The last example lists over 6,000 Flagstar employees' information, including their salaries, 401K allocations, home addresses, employee ID numbers, ages, tenure at Flagstar, office locations, and divisions.

60. As another example, a document posted on the dark web from Flagstar's FTA platform lists the name, date of birth, age, credit score, driver's license number, mother's maiden name, relatives, previous addresses, email addresses, email password, employment history, account numbers and balances, and security questions and answers for certain accounts for a customer with a Flagstar mortgage. This is the holy grail of identity theft, and it is unclear why Flagstar would aggregate these data points into one document and then store it, unredacted and unencrypted, on a file transfer platform.

## IV. Flagstar Issued Late and Deficient Notices to Consumers.

61. Although Flagstar learned of the first cyberattacks on December 23, 2020, and then learned of the breach of Flagstar's FTA platform on January 22, 2021, Flagstar did not publicly disclose the breach until March 5, 2021. On that date, Defendant posted an announcement on its website generally stating that certain "information" was impacted. Defendant's public statement read:

> 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. After Accellion informed us of the incident, 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.

62. 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 confirms the information exposed in the Data Breach was not limited to names, Social Security numbers, home addresses and phone numbers, but also included dates of birth and/or financial account numbers.[75]

63. It was not until March 15, 2021 that consumers were finally notified that the data breach involved the Social Security numbers and other sensitive PII of its customers. On or around that date, Defendant sent Plaintiffs and Class Members

[75] *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").

a *Notice of Data Breach*.[76] Defendant generally informed Plaintiffs and Class Members as follows:[77]

> ***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?***

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

[77] The *Notice of Data Breach* varies as to whether data elements other than Social Security number were exposed, such as account number.

> 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.[78]

64. Flagstar's delay in notifying its customers of the Data Breach for over five weeks, particularly when Flagstar knew it was likely that some or all of that data would be posted on the dark web at the conclusion of its ransom negotiations, was patently unreasonable and prevented Plaintiffs and Class Members from taking steps to protect themselves against identity theft and fraud sooner.

65. Although this letter stated that Flagstar "discontinued use" of the FTA platform, it does not state that Flagstar changed its other deficient security practices that resulted in the data breach, such as indefinite retention of customer data; inappropriate indefinite storage of customer data on file transfer platforms; insufficient vendor management practices; and lack of data encryption on Flagstar's

[78] *Id.* at 1–2.

servers, among other things. Upon information and belief, Flagstar continues to engage in these and other deficient security practices.

66. Flagstar has failed to explain why documents containing 1.4 million customers and employees' PII were being stored on the FTA platform, which was intended for use as a file share platform, instead of or in addition to Flagstar's data warehouse or other internal servers that Flagstar has represented to be "segmented" from the FTA platform.

67. Flagstar failed to search for, identify, or disclose to impacted individuals the full extent of PII that was exfiltrated in the Data Breach. As one known example, Flagstar informed Plaintiff Moniz that his Social Security number, date of birth, first name, and last name were exfiltrated in the Data Breach. However, a document pulled from the CLOP dark web posting reveals Plaintiff Moniz's home address was also in the impacted dataset alongside his name and other personal information.

68. Further, other than what can be gleaned from individual notice letters, Flagstar has not disclosed the specific "data elements" for each consumer that it chose to search for in the exfiltrated documents for purposes of disclosure in the notice letters. Recent statements by Flagstar's Chief Information Officer, Jennifer Charters, suggest that Flagstar did not search for at least some sensitive data elements like signatures.

69. Flagstar has also failed to disclose enough information to allow impacted individuals to determine, for themselves, what types of personal information were exposed in the data breach other than the discrete "data elements" listed on the notice letters. Indeed, although Flagstar's customers routinely disclose to Flagstar information such as (1) full address histories (2) multiple email addresses (3) multiple phone numbers (4) numerous financial account numbers, etc., Flagstar's notice letter failed to describe with any particularity *which* email address, account number, etc. was subject to the breach for any given individual. Although Flagstar told impacted individuals that "one or more of the documents removed from the Accellion platform" contained their PII, Flagstar failed to disclose what type of document or document(s) were stolen for impacted individuals, given that thousands of mortgage and loan applications were stolen in the breach, which are "treasure troves" of information for cyber criminals. Further, given that full documents were stolen in the data breach—not just discrete data points—Flagstar has also failed to disclose to consumers the probability that other "non-PII" data elements were disclosed alongside their PII.

70. Flagstar's notice letter is also misleading. It states: "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 third party. Flagstar permanently discontinued use of this file sharing platform." These

statements falsely imply that January 22, 2021 was the first time Accellion notified Flagstar that an unauthorized third party exploited a vulnerability in the system when Accellion had, in fact, notified Flagstar of this fact on December 23, 2020.

71. Flagstar's notice letter also states "we acted immediately to contain the threat[.]" This statement falsely implies that Flagstar acted immediately in light of the cyberattack on the FTA platform when it had, in fact, failed to take appropriate action in response to several critical events, including but not limited to when Flagstar (1) learned the FTA platform was no longer receiving security updates; (2) learned the FTA platform's operating system was end-of-life; and (3) learned the FTA platform was under attack by cybercriminals on December 23, 2020.

72. Flagstar's notice letter also states that "[u]pon learning of the vulnerability, Flagstar promptly took the Accellion server offline and permanently discontinued use of this file sharing platform[.]" This statement falsely implies that the decision to discontinue use of the FTA platform was timely when, in fact, Flagstar had prior knowledge that the FTA was an obsolete and dangerous product and yet failed to act. This statement also falsely implies that the decision to discontinue use of the FTA provided a benefit to customers and employees affected by the breach, when, in reality, the decision to discontinue use of the FTA was made too late, after Plaintiffs' PII had been exfiltrated, and had no impact on the vast amounts of PII exposed.

## V. The Data Breach was Flagstar's First of Two in a Single Year.

73. The Data Breach and resulting harm suffered by Plaintiffs and Class Members is directly attributable to Flagstar's security lapses and data mismanagement. Flagstar continues to engage in deficient data security and vendor management practices. This is evidenced by the two subsequent data breaches experienced by Flagstar in 2021 and 2023.,

74. The instant Data Breach is the first of two major incidents to impact Flagstar and its customers in a single year. From November 2021 through December 2022, Flagstar suffered a second data breach compromising the PII of over 1.5 million former and current Flagstar customers. Flagstar waited until June 17, 2022, six months after the breach, to disclose that breach to impacted individuals, consumers, and the public.

75. Then, in May 2023, Flagstar experienced a third breach, again by CLOP leveraging a third-party file transfer vendor, which involved the exfiltration of 837,390 customers' PII.

76. Flagstar's failure to employ appropriate data security and vendor management practices puts Plaintiffs' PII continually at risk. The cybersecurity threats to the financial industry remain critical. According to the IBM 2023 Threat Index, Financial Services Sector entities have experienced either the most or second most cyber incidents for each of the past five years, while the 2024 Homeland

Security Threat Assessment highlights financial services as one of the sectors Chinese government cyber actors are likely to continue targeting.[79]

## VI. Flagstar's Use of the FTA Platform Was Highly Dangerous.

77. On February 25, 2021, Accellion announced that it was accelerating the end of life for the FTA, effective April 30, 2021. On May 18, 2021, Accellion issued a press release stating that "As of May 18, 2021," 75% of FTA customers impacted by the breach had migrated to Kiteworks.

78. Flagstar knew or should have known, before the Data Breach, that the FTA did not have adequate security features because Accellion made security deficiencies of the FTA—like, among other things, its lack of encryption for "at rest" data and its lack of compliance with certain security regulations—known to customers.

79. By way of example, on a webpage titled "FTA/Accellion Platform Comparison," Accellion published a table that demonstrated a "feature-by-feature comparison" of the FTA (left column) to the Kiteworks platform (right column), including, among other things:[80]

---

[79] *See Homeland Threat Assessment 2024*, DEPARTMENT OF HOMELAND SECURITY, *available at* https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf (last accessed May 13, 2024).

[80] *FTA/Accellion Platform Comparison*, ACCELLION.COM (as of Aug. 7, 2020), *available at*

| Protection from External Threats | | |
|---|---|---|
| AV scan incoming emails and Accellion uploads | ✓ | ✓ |
| AV scan enterprise content source up/downloads | | ✓ |
| ATP scan on all incoming files: Check Point SandBlast, FireEye Malware Analysis (AX), ICAP | | ✓ |
| Mime-type (e.g., .exe) exclusion controls | | ✓ |
| Intrusion detection system (IDS) | ✓ | ✓ |
| TLS 1.2 encryption in transit | ✓ | ✓ |
| AES-256 Encryption at rest | | ✓ |
| Admin can disable individual SSL ciphers | | ✓ |
| Hardware Security Module (HSM) integration | | ✓ |

| US Federal Standards | | |
|---|---|---|
| Section 508 | ✓ | ✓ |
| FIPS 140-2 | Deprecated | ✓ |
| FedRAMP | | ✓ |

80. In FAQs published in spring of 2021, Accellion explained how the Kiteworks' platform was "different" from the FTA platform: "The Kiteworks content firewall platform was unaffected by these attacks. It is built on a completely different codebase, using state-of-the-art security architecture and devops security processes. Kiteworks software is updated on an agile quarterly release cycle, undergoes extensive penetration testing on a regular basis, and has FedRAMP-compliant hosting options…."

---

https://web.archive.org/web/20200807032115/https://www.accellion.com/products/fta-comparison/ (last accessed May 13, 2024).

81. In an interview in 2021, Joel York, Accellion's Chief Marketing Officer, confirmed that the Data Breach involved a "legacy" FTA product which the company had been advising customers "for years" to stop using. As a legacy product, York stated: the FTA "just wasn't designed for these types of threats."[81]

82. After the breach, Accellion published a blog to ensure that its own clients were practice vendor risk management, reemphasizing that their customers should have vetted and protected themselves from third party vendors that "come into contact with critical business operations and information" and "even vendors that have the best operational and logistical support, introduces risk into your business: risk of breach, inefficiency, or loss or damage to data."[82]

83. Flagstar's continued use of the FTA platform despite the known and obvious risks posed to customer PII demonstrates a clear failure to employ appropriate vendor management practices. Oliver Tavakoli, CTO at Vectra, said the cyberattacks were "portable and required little customization because the purpose of

[81] Jim Brunner, *Banking, Social Security info of more than 1.4 million people exposed in hack involving Washington state auditor*, SEATTLE TIMES (Feb. 1, 2021), *available at* https://www.seattletimes.com/subscribe/signup-offers/?pw=redirect&subsource=paywall&return=https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/ (last accessed May 7, 2024).

[82] *The Importance of Vendor Risk Management for CISOs*, KITEWORKS.COM, (July 27, 2023), *available at* https://www.kiteworks.com/third-party-risk/the-importance-of-vendor-risk-management-for-cisos/?source=boilerplatePR (last accessed May 13, 2024).

Accellion's FTA was to transfer large [] data" and serve as a reminder that security teams need to be "keenly aware" of the third-party tools they use, particularly with sensitive data—he explained: "[w]hen the vendor who supplies such a product spends 3 years trying to coax you to their new product, you may want to consider the subtext of that communication."[83]

84. Flagstar's continued use of the FTA platform despite the known dangers of using legacy and end-of-life software is particularly egregious. According to Karen Walsh, CEO of Allegro Solutions, the Data Breach was yet "another example of cybercriminals looking to exploit end-of-life tools." Given that the FTA's operating system CentOS 6, was no longer supported as of November 30, 2020, Walsh explained: "FTA customers were running a service that relied on a now-unsupported technology."[84]

85. Legacy systems are "low-hanging fruit" for cyber criminals, and Flagstar knew or should have known of the dangers of using the FTA platform well before the Data Breach. "Imagine buying a hundred-year-old house. To keep your

[83] Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC (Feb. 24, 2021), *available at* https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/ (last accessed May 8, 2024).
[84] Jonathan Greig, *Kroger data breach highlights urgent need to replace legacy, end-of-life tools*, TECHREPUBLIC (Feb. 24, 2021), *available at* https://www.techrepublic.com/article/kroger-data-breach-highlights-urgent-need-to-replace-legacy-end-of-life-tools/ (last accessed May 8, 2024).

family safe, you need to update the antiquated plumbing and electrical systems to meet current building standards. But there's no existing blueprint to guide the work, and you need to keep the lights on and the water flowing during the renovation process. This scenario mirrors the hurdles that organizations face with legacy IT systems—outdated computer hardware, applications or methods that continue to be used."[85]

86. "For example, to support specific business processes, an organization might continue to use an old operating system like Windows 7, an old database system like Oracle 8i or SQL Server 2000, or deprecated authentication, encryption, or network protocols. Like the utilities in the old house, these legacy IT systems are actively being used, so organizations can't easily discard them. But they require significant overhaul to meet today's compliance and security standards—a process that is both challenging and fraught with risk."[86]

87. The inherent risks in using legacy products has resulted in "plenty of documented cyberattacks in which a legacy…IT system was the source of a major

[85] Dirk Schrader, *Mitigating the security risks of legacy IT systems*, SECURITYINFOWATCH.COM (Jan. 10, 2024), *available at https://www.securityinfowatch.com/cybersecurity/article/53081992/mitigating-the-security-risks-of-legacy-it-systems* (last accessed May 8, 2024).
[86] Dirk Schrader, *Mitigating the security risks of legacy IT systems*, SECURITYINFOWATCH.COM (Jan. 10, 2024), *available at* https://www.securityinfowatch.com/cybersecurity/article/53081992/mitigating-the-security-risks-of-legacy-it-systems (last accessed May 8, 2024).

breach."[87] "Continuing to use legacy IT systems also puts the organization at risk of compliance violations [for failing to] take appropriate measures to mitigate security risks[.]"[88]

88. So too for EOL software. "Part of a proactive security approach is ensuring that your company is never running on end of life (EOL) software – whether you're a provider of the software or on the receiving end."[89] "Running EOL versions of any software can pose a substantial risk and cause failure in IT internal and external compliance."[90]

89. On February 1, 2021, the Cybersecurity and Infrastructure Security Agency (CISA), established under section 2202 of the Homeland Security Act of 2002 (6 U.S.C. § 652), issued a press release announcing it was developing a catalog of "Bad Practices" that "are exceptionally risky, especially in organizations supporting Critical Infrastructure[.]"[91] The number one "Bad Practice," according to

---

[87] *Id.*
[88] *Id.*
[89] *In the Line of Fire: Addressing Vulnerabilities in Your Legacy Software*, VERIMATRIX CYBERSECURITY (Apr. 26, 2021), *available at* https://www.securityinfowatch.com/cybersecurity/article/53081992/mitigating-the-security-risks-of-legacy-it-systems (last accessed May 8, 2024).
[90] Javier Perez, *The Great CentOS Linux Migration: How We Got Here and What's Next*, DEVOPS.COM (Sept. 8, 2023), *available at* https://devops.com/the-great-centos-linux-migration-how-we-got-here-and-whats-next/ (last accessed May 8, 2024).
[91] *Press Release: Bad Practices*, CYBERSECURITY INFRASTRUCTURE & SECURITY AGENCY (Feb. 1, 2021), *available at* https://www.cisa.gov/news-events/news/bad-practices-0 (last accessed May 8, 2024).

CISA, is the "[u]se of unsupported (or end-of-life) software in service of Critical Infrastructure," which CISA states "is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in technologies accessible from the Internet."[92] According the CISA, "[t]he presence of these Bad Practices in organizations that support Critical Infrastructure"—like Flagstar—"is exceptionally dangerous and increases risk to our critical infrastructure, on which we rely for national security, economic stability, and life, healthy, and safety of the public."[93]

90. Indeed, Flagstar has repeatedly acknowledged the need to use up-to-date software to protect customers' PII. Emphasizing that its customers' personal information is "**a target**,"[94] Flagstar advises its customers to protect their identities and prevent fraud by using up-to-date systems, stating that "[o]ne of your greatest defenses against online security threats is to make sure your computer and mobile device have security software… Make sure your programs are up to date and running the latest version[,]" and "[u]pdate your software and operating system on a regular

[92] *Id.*
[93] *Id.*
[94] *Protecting Your Identity*, FLAGSTAR.COM, *available at* https://www.flagstar.com/personal/learn/learning-hub/protecting-your-identity/cyber-safety.html (last accessed May 8, 2024).

basis[.]"[95] Flagstar warns, "[r]apid advances in technological and creative criminal minds make fraud a potentially serious threat on a variety of fronts."[96] Yet Flagstar failed to heed its own basic advice and instead used an out-of-date platform on an end-of-life operating system to store customer data.

91. Flagstar knew or should have known of the dangers of using the FTA. Flagstar had an admitted responsibility to practice third-party risk management, and Flagstar had the resources and information necessary to anticipate and address the obvious security risks posted by the FTA, including a full suite of professionals tasked with maintaining the company's systems, including Chief Information Security Officer, Vendor Management Department, and Information Security Department. Yet Flagstar failed to take appropriate steps to protect the PII of Plaintiffs and Class Members.

## VII. Flagstar's Failure to Implement Safeguards to Protect PII was Egregious.

92. Flagstar was one of only a subset of remaining FTA customers that were impacted by the cyberattacks.[97] Of the 320 remaining FTA customers at the

[95] *Id.*; *see also Preventing Fraud*, FLAGSTAR.COM, *available at* https://www.flagstar.com/fraud-information-center/preventing-fraud.html (last accessed May 8, 2024).
[96] *Id.*
[97] *Accellion FTA Attack Customer FAQs*, ACCELLION (March 1, 2021), *available at* https://www.kiteworks.com/sites/default/files/trust-center/accellion-fta-attack-customer-faqs.pdf (last accessed May 8, 2024).

time of the breach, under 100 were victims of the attack, and only around 25, including Flagstar, suffered significant data theft.[98]

93. The fact that Flagstar's data was viewable and removable by cyber criminals once they had access to the FTA was due to Flagstar's failure to institute basic measures to protect Plaintiffs' PII on the FTA product. Had Flagstar properly secured and encrypted the PII of Plaintiffs and Class Members, used proper firewalls, or destroyed unnecessary data from the system, Plaintiffs would not have been harmed.

94. The Accellion FTA server, according to standard implementations, would have been present within Flagstar's network and should have been placed behind a firewall to detect non-authorized access. In addition, the attacker would have to have known Flagstar used the Accellion FTA application and service. Currently, the subdomain enumeration shows that Flagstar has a subdomain of kiteworks.test.flagstar.com, therefore it is reasonable to assume that Flagstar configured the previous service, FTA, in the same manner and the FTA service would have been easily discovered by threat actor scans of the public internet. Upon

[98] Tara Seals, *Accellion FT Zero-Day Attacks Show Ties to Clop Ransomware, FIN11*, THREAT POST (Feb. 22, 2021), *available at* https://threatpost.com/accellion-zero-day-attacks-clop-ransomware-fin11/164150/ (last accessed May 8, 2024); *see also* https://www.recordedfuture.com/blog/dewmode-accellion-supply-chain-impact.

information and belief, Flagstar failed to incorporate firewalls, which allowed the cyber criminals to both access and exfiltrate Plaintiffs' PII.

95. Further, Flagstar failed to encrypt or even password-protect the documents and data stored on the FTA server. Although the FTA purported to encrypt data in transit, Flagstar knew (or should have known) that the FTA did not encrypt the data "at rest" on Flagstar's server. Encrypting data in transit *and* at rest is vital to keeping it secure.[99] "Critical security and governance capabilities must include….[e]ncryption of PII like social security numbers, credit scores, transaction records, etc., in transit and at rest."[100] "Secure file sharing for banks is achieved with…encryption of content in transit and at rest."[101] Yet Flagstar failed to encrypt PII at rest in the FTA, which allowed the cyber criminals to exfiltrate and view Plaintiffs' PII.

---

[99] *DevSecOps: Integrate Data Security Into the Software Development Life Cycle*, KITEWORKS.COM, *available at* https://www.kiteworks.com/risk-compliance-glossary/devsecops-integrate-data-security-into-the-software-development-life-cycle/ (last accessed May 8, 2024).

[100] Bob Ertl, *Secure File Sharing in Banking Amid Industry Disruption: New Model, New Challenges*, ACCELLION.COM (July 18, 2017), *available at* d https://web.archive.org/web/20201029144423/https:/www.accellion.com/blog/secure-file-sharing-in-banking-new-universal-banking-model/ (last accessed May 12, 2024).

[101] Bob Ertl, *OCC 2013-29 Compliance: Why Secure File Sharing for Banks Needs to Include Partners*, ACCELLION.COM (Sept. 26, 2018), *available at* https://web.archive.org/web/20201022201024/https:/www.accellion.com/blog/occ-2013-29-compliance-why-secure-file-sharing-for-banks-needs-to-include-partners-2/ (last accessed May 12, 2024).

96. Flagstar also failed to "clean out" unneeded files from the FTA system and left unencrypted documents and data containing sensitive PII stored there for years without justification. As one article explained, the cyberattacks "highlight the importance of data storage issues and records retention requirements."[102] "Some of the impacted companies may discover that they could have minimized their risks by moving their files off the FTA platform once they had been downloaded by the recipient."[103]

97. Here, Flagstar had no legitimate purpose for storing such mass quantities of PII on the FTA platform. Not only was the platform intended only for temporary file sharing and was not appropriate for use as an enterprise-level data storage system, but Flagstar had actual data storage systems in place. For example, Flagstar had, and has, a dedicated "data warehouse" that houses all of Flagstar's customer data, which is seemingly "segmented" from the FTA platform. By using the FTA as a functional information repository, Flagstar substantially increased the volume of information at risk.

---

[102] *Third Party Risk Management Lessons Learned from Recent Accellion Breach*, TEAM CENTRL (Mar. 19, 2021), *available at* https://www.centrl.ai/resources/third-party-risk-management-lessons-learned-from-recent-accellion-breach/ (last accessed May 8, 2024).

[103] *Id.*

98. These basic security failings demonstrate that Flagstar again failed to heed the basic advice and warnings Flagstar provides to its own customers.[104] Flagstar was at all times fully aware of its obligation to protect the PII of Flagstar's former and current customers and employees. Flagstar was also aware of the significant repercussions if it failed to do so because Flagstar collected PII from millions of consumers and it knew that this PII, if hacked, would result in injury to consumers, including Plaintiffs and Class Members.

99. By failing to address these basic security failings, Flagstar also failed to comply with the "key pillars" of its own information security program: "Identify, Protect, Detect, Respond, and Recover."[105]

## VIII. Flagstar Said Nothing About the Danger to Plaintiffs' PII.

100. At all relevant times, Flagstar has known that its data storage practices are highly dangerous.

101. Plaintiffs could not reasonably have known of, and could not be reasonably expected to discover, the deficiencies in Flagstar's data management

---

[104] To prevent identity theft, Flagstar advises its customers that it should destroy documents containing PII that are no longer needed ("**Get rid of it**") and to store important information like passwords in "encrypted" password managers. *Protecting Your Identity*, FLAGSTAR.COM, *available at* https://www.flagstar.com/personal/learn/learning-hub/protecting-your-identity/cyber-safety.html (last accessed May 8, 2024).

[105] *Data Security and Customer Privacy*, WWW.FLAGSTAR.COM, https://www.flagstar.com/esg/governance/data-security-and-customer-privacy.html (last visited May 6, 2024).

practices *unless* Flagstar disclosed them. *See, e.g., In re Rutter's Inc. Data Sec. Breach Litig.*, 511 F. Supp. 3d 514, 543 (M.D. Pa. 2021) ("When a meat processor says nothing about the safety of its meat, one can justifiably conclude from that silence that the meat contains no harmful bacteria[.]").

102. Flagstar had a duty to disclose material facts to Plaintiffs (that were in Flagstar's exclusive control) regarding Flagstar's deficient data security practices, including Flagstar's use of an unsecure file transfer platform without requisite encryption or clearinghouse practices. Flagstar knew or should have known that the undisclosed information about the security of Plaintiffs' PII was material to Plaintiffs' decision to conduct business with Flagstar. In fact, "[m]ost consumers consider privacy and data protection a major factor when choosing a financial services company."[106]

103. Flagstar said nothing to consumers about its poor data management practices at the time the customer relationship was formed, or any time thereafter.

104. Flagstar intended that Plaintiffs rely on its silence as grounds to believe that their PII was appropriately safeguarded.

105. Plaintiffs reasonably relied on Flagstar's silence as grounds to believe that their PII was appropriately safeguarded.

---

[106] Penny Crosman, *Flagstar's data breach, and what we can learn from it*, AMERICAN BANKER (Mar. 15, 2021).

106. By failing to address and disclose these basic security failings, Flagstar made material misrepresentations to Flagstar customers and the public in its website and Privacy Policy, including: "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[107]

## IX. Flagstar Failed to Comply with Federal Law, Regulatory Guidance, and Industry-Standard Cybersecurity Practices.

### A. Flagstar's Conduct Violates Section 5 of the FTC Act.

107. Flagstar failed to comply with Federal Trade Commission ("FTC") guidance on protecting PII and industry-standard cybersecurity practices. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

108. The FTC recommends:

a. limiting access to customer information to employees who have a business reason to see it;

[107] *Id.*

b. keeping customer information in encrypted files provides better protection in case of theft;

c. maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information;

d. using appropriate oversight or audit procedures to detect the improper disclosure or theft of customer information;

e. monitoring both in- and out-bound transfers of information for indications of a compromise, such as unexpectedly large amounts of data being transmitted from your system to an unknown user; and,

f. monitoring activity logs for signs of unauthorized access to customer information.[108]

109. The FTC has also issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[109]

110. In 2016, the FTC updated its publication, *Protecting PII: A Guide for Business*, which established guidelines for fundamental data security principles and

[108] FEDERAL TRADE COMMISSION, *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, available at https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

[109] FEDERAL TRADE COMMISSION, *Start With Security* at 2, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

practices for business.[110] The guidelines note businesses should protect the personal customer information that they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

111. The FTC recommends that businesses delete payment card information after the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

112. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the

[110] FEDERAL TRADE COMMISSION, *Protecting PII: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

113. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

114. The FTC has interpreted Section 5 of the FTC Act to encompass failures to appropriately store and maintain personal data.

115. Flagstar was fully aware of its obligation to implement and use reasonable measures to protect the PII of its customers, including the need to encrypt customer data on their computer networks, but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Flagstar's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

**B. Flagstar's Conduct Violates State Laws on Data Security.**

116. Defendant has also violated the laws of at least 24 states that require that businesses that own, license or maintain PII implement and maintain

"reasonable security procedures and practices" and to protect PII from unauthorized access. California is one such state and requires that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification or disclosure." Cal. Civ. Code § 1798.81.5(b).

**C. Flagstar's Conduct Violates the GLBA.**

117. Defendant also violated the Gramm-Leach-Bliley Act. 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.

118. 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).

119. 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.

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

121. 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.

122. 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 Accellion FTA.

123. Defendant also failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on Accellion FTA and would do so after the customer relationship ended.

124. 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.

125. Defendant failed to (1) assess reasonably foreseeable risks to the security, confidentiality, and integrity of the customer information on the FTA platform (2) design or implement safeguards to control those risks; (3) oversee Accellion; and (4) evaluate and adjust its practices in light of several critical events.

126. 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."

127. 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."

128. As of January 4, 2019, Defendant admitted that it had not provided

Plaintiffs or Class Members an opt-opt 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."

129. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class Members using the FTA platform without providing Plaintiffs and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

130. Defendant has not informed Plaintiffs and Class Members of the reason Defendant shared the PII of more than 1.4 million individuals using Accellion FTA; if this was done to share the PII with a 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.

### D. Flagstar's Conduct Violated Regulations and Guidance on Data Breach Notifications to Consumers.

131. Further, in a ruling that took effect in May 2022, the Federal Deposit Insurance Corp. (FDIC), the Office of the Comptroller of the Currency (OCC), and the Federal Reserve (together, the "agencies") now require banks to notify their primary federal regulator within 36 hours of determining whether a "significant computer-security incident" could disrupt business or the stability of the financial sector, and requires banks to inform affected bank customers "as soon as possible,"

recognizing cyberattacks targeting the financial services industry "have increased in frequency and severity in recent years."[111] Flagstar violated this ruling by delaying notifying its customers of the cyber-attack for weeks after it occurred, preventing them from taking steps to protect themselves against fraud and identity theft sooner.

## X. The Impact of the Data Breach on Plaintiffs and Class Members.

132. Flagstar's failure to keep Plaintiffs' and Class Members' PII secure has severe ramifications. Given the sensitive nature of the PII stolen in the Data Breach—names, Social Security numbers, account and loan numbers, etc.—cyber criminals can commit identity theft, financial fraud, and other identity-related fraud against Plaintiffs and Class Members now and into the indefinite future. As a result, Plaintiffs have suffered injury and faced an imminent and continued risk of further injury for the remainder of their lives, including identity theft and related cybercrimes due to the Data Breach.

133. It is no wonder Plaintiffs' stolen PII is circulating on the dark web, as it is highly valuable. Stolen PII is one of the most valuable commodities on the criminal information black market. For example, one source reports that personal

[111] *Fed, FDIC, OCC approve 36-hour window for reporting cyberattacks*, BANKING DIVE, *available at* https://www.bankingdive.com/news/36-hour-window-fed-fdic-occ-cybersecurity-technology-vendor/592275/ (last accessed June 16, 2023); FEDERAL RESERVE, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, available at https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211118a1.pdf (last accessed June 16, 2023).

information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[112] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[113] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[114] According to Martin Walter, senior director at cybersecurity firm RedSeal, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[115]

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

---

[112] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed September 12, 2023).

[113] *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 September 12, 2023).

[114] *In the Dark*, VPNOVERVIEW (2019) *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed September 12, 2023).

[115] 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 September 12, 2023).

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.[116]

135. 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. Even then, a new Social Security number may not be effective. Even new Social Security numbers typically must be linked to the previous Social Security number for most people with established credit or those over the age of 18. 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

[116] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 12, 2023).

number."[117]

136. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee.

137. Popular marketplaces and forums, often the subject of monitoring and review by credit identity theft services, law enforcement, and threat intelligence professionals, are typically not the first-place stolen data is aggregated and sold. By the time an individual's stolen PII makes it to an auction or online sale site, it usually has already been used, sold for higher prices, or has been broken up into pieces of the data on other forums and markets, also known as secondary sites.

138. Stolen data sources have relatively long shelf lives especially if the data is immutable. The lifecycle of data sold or shared on the darknet and similar criminal marketplaces (not all sites are located on the darknet) is circuitous. Stolen data is often used to propagate future attacks. Each future breach renews the shelf life because it embellishes and organically validates the original data.

139. Armed with the PII acquired in this type of cyberattack, threat actors can commit a variety of crimes, including identity theft, which the Federal Trade

[117] 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 September 12, 2023).

Commission ("FTC") defines as "a fraud committed or attempted using the identifying information of another person without authority."[118]

140. One such example of criminals using PII for profit is the development of "Fullz" packages.[119] Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

141. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone

[118] 17 C.F.R. § 248.201 (2013).

[119] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information one has on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sept. 18, 2014), https://krebsonsecurity.com/tag/fullz/.

numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and other Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

142. Malicious actors can use the information stolen in the Data Breach as a foundation for reconnaissance and stratifying potential victims. Having the confidential PII allows for impersonation, which allows bad actors to gain additional information about the stolen entity. For example, a criminal can use www.creditkarma.com to register using the stolen identifying information and find out if a credit freeze was implemented, learn about the credit history of the stolen identity, and more. Sites like Credit Karma require the following fields that were stolen as part of the breach: home address, SSN, DOB, information about employment, current mortgage holder and other general information. The "free" report will indicate credit cards, mortgage, amount owed, and with a full account, personal information may be changed. This is often how threat actors will validate the data and then sell each verified record at a higher price.

143. Malicious actors can use PII to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can use consumers' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."[120]

144. For example, "[i]f fraudsters have your full name and SSN," Identity Guard warns, "they could apply for loans or access your bank accounts."[121] Further, "[h]ackers can use your PII in phishing scams to trick you into revealing more sensitive information."[122]

145. According to the FDIC's Cyber Fraud and Financial Crimes Section, "[s]mall transactions on an account might be signs that someone has learned your account information and issuing it to commit a crime…. That's why it's important to be on the lookout for fraudulent transactions, no matter how small."[123] In one example, the FTC alleged that a group of individuals stole nearly $10 million by

[120] A criminal combines real and fake information to create a new "synthetic" identity, which is used to commit fraud.

[121] *What Data Do Cybercriminals Steal?*, IDENTITY GUARD (Feb. 14, 2024), *available at* https://www.identityguard.com/news/what-information-do-cyber-criminals-steal#:~:text=When%20cybercriminals%20steal%20PII%2C%20they,harder%20for%20authorities%20to%20detect(last visited May 7, 2024).

[122] *Id.*

[123] *When Small Charges Can Signal a Big Crime*, FDIC (2016).

making charges to more than a million credit and debit cards that went unnoticed by most of cardholders because the transactions ranged from 20 cent to $10.[124]

146. Further, data breaches that expose any personal data, and in particular nonpublic data of any kind (e.g., salary, donation history), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future. Spear phishing results in a high rate of identity theft, fraud, and extortion.

147. Malicious actors often wait months or years to use the PII obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[125]

148. These bad actors will also re-use stolen PII, meaning individuals can be the victim of several cybercrimes stemming from a single data breach.

149. Moreover, there is often a significant time lag between when a person

---

[124] *Id.*

[125] U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* 42 (June 2007), available at https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-07-737/html/GAOREPORTS-GAO-07-737.htm (last visited June 16, 2023).

suffers harm due to the theft of their PII and when they discover the harm. Plaintiffs will therefore need to spend time and money to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

150. Plaintiffs and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of Flagstar's Data Breach. In other words, Plaintiffs have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Breach.

151. To date, Defendant has offered Plaintiffs and Class Members only two years of identity monitoring through a single provider, Kroll. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they will face for years to come, particularly in light of the nature of the PII disclosed.

152. Plaintiffs and Class Members have also realized harm in the lost or reduced value of their PII. Flagstar admits the PII compromised in the Breach is valuable. As discussed above, Flagstar collects, retains, and uses Plaintiffs' PII to increase profits. Plaintiffs' PII is not only valuable to Flagstar, but Plaintiffs also

place value on their PII based on their understanding that their PII is a financial asset to companies that collect it.[126]

153. Plaintiffs and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to Plaintiffs' PII that was permitted without authorization by Flagstar. This market value for access to PII can be determined by reference to both legitimate and illegitimate markets for such information.

154. Moreover, Plaintiffs and Class Members value the privacy of this information and expect Flagstar to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Flagstar or provided their PII had they known Flagstar did not implement reasonable security measures to protect their PII.[127] Customers reasonably expect that the payments they

---

[126] *See, e.g.*, *Ponemon Institute, LLC, Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers* at p. 14 (March 2015) available at https://docplayer.net/836701-Privacy-and-security-in-a-connected-life-a-study-of-us-european-and-japanese-consumers.html (explaining that 53% of respondents "believe personal data is a financial asset similar to traded goods, currencies or commodities" and valuing, as but one example, their Social Security number at $55.70).

[127] FIREEYE, *Beyond the Bottom Line: The Real Cost of Data Breaches* (May 11, 2016), https://www.fireeye.com/current-threats/cost-of-a-data-breach/wp-real-cost-data-breaches.html (noting approximately 50% of consumers consider data security to be a main or important consideration when making purchasing decisions and nearly the same percentage would be willing to pay more in order to work with a provider that has better data security. Likewise, 70% of consumers would provide less PII to organizations that suffered a data breach).

make for Flagstar's services incorporate the costs to implement reasonable security measures to protect customers' PII. And because consumers value data privacy and security, companies with robust data security practices can command higher prices than those who do not. As a result, Plaintiffs and Class Members did not receive the benefit of their bargain with Flagstar because they paid a value for services they expected but did not receive.

155. Given Flagstar's failure to protect Plaintiffs' and the Class Members' PII despite a data breach earlier that same year, Plaintiffs have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages, restitution, or disgorgement) that protects them from suffering further harm, as their PII remains in Flagstar's possession. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

## XI. Plaintiffs' Experiences.

156. Plaintiffs place significant value in the security of their PII. Plaintiffs agreed to entrust their sensitive PII to Flagstar with the understanding that Flagstar would keep their information secure and employ reasonable and adequate security measures to ensure that it would not be compromised. If Plaintiffs had known of Flagstar's lax and totally inadequate security practices with respect to Plaintiffs' PII, they would not have done business with Flagstar, would not have applied for and/or

consented to Flagstar's provision of services, would not have opened, used, or applied for Flagstar's services at the applicable rates and on the applicable terms, or would have paid less because of the diminished value of Flagstar's services.

157. 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. As a 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.

158. Plaintiffs and Class Members have suffered injury as a result of Flagstar's conduct. These injuries include: (1) lost or diminished value of PII; (2) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (3) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (4) the continued and increased risk to their PII, which remains unencrypted and available for unauthorized

third parties to access and abuse and may remain backed up in Flagstar's possession and is subject to further unauthorized disclosures so long as Flagstar fails to undertake appropriate and adequate measures to protect the PII.

**A. Plaintiff Philip Angus**

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

160. In 2014, Plaintiff Angus obtained a residential mortgage loan from Defendant for a home in Florida. In connection with his loan application, Plaintiff Angus provided financial and other highly sensitive information to Defendant, including his Social Security Number.

161. In or around October 2015, Plaintiff Angus's loan was sold to a different entity. More than five years after the customer relationship with Defendant ended, Defendant stored and/or shared some of Plaintiff Angus's most sensitive (and extremely valuable to cyber criminals and identity thieves) PII using Accellion FTA, resulting in the exposure of Plaintiff Angus's PII during the Data Breach.

162. As of June 9, 2023, Plaintiff Angus's loan is back with Flagstar.

163. On or around March 15, 2021, Plaintiff Angus learned of the Data Breach via the *Notice of Data Breach* letter that Defendant sent to Plaintiff Angus on or around that date. In the letter, Defendant informed Plaintiff Angus that document(s) containing his Social Security number, full name, phone number, and

home address were "removed" from the FTA platform by unauthorized actors during the Data Breach.

164. Flagstar has not explained why document(s) containing Plaintiff Angus's PII were being stored or shared on the FTA platform more than five years after Plaintiff Angus's customer relationship with Defendant ended.

165. Although Flagstar told Plaintiff Angus that "one or more documents removed from the Accellion platform" contained his PII, Flagstar has not disclosed to Plaintiff Angus what those document(s) are, nor has Flagstar explained whether those documents contain other information regarding Plaintiff Angus besides the "data elements" Flagstar listed in the notice letter.

166. As a result of the Data Breach, Plaintiff Angus purchased a monthly subscription for credit monitoring services through Experian. For the first two years, Plaintiff Angus paid approximately $19.99 a month for this service, and he continues to pay $5.00 a month for this service to date. Since the Data Breach, Plaintiff Angus has received notices from Experian that his phone number and Social Security number are on the dark web.

167. As a result of the Data Breach, Plaintiff Angus purchased a 3-year subscription to HomeLock, a property fraud protection service, for $199.

168. As a result of the Data Breach, Plaintiff Angus experienced a significant increase in the volume of phishing and scam calls he receives, including calls from

individuals asking for his bank account details and other personal information. These calls would occur frequently at night, particularly after 5:00pm, and would often force Plaintiff Angus to disconnect his phone. Because of the increase in phishing and scam calls after the Data Breach, Plaintiff Angus conducted substantial research on how to filter or block unwanted calls, and ultimately purchased a subscription for a VoIP Phone System for approximately $10.00 a month. Plaintiff Angus continues to pay for this service.

169. After the Data Breach, Plaintiff Angus was notified by his bank that an unauthorized individual in a foreign country was attempting to use his account to make a purchase. Plaintiff Angus's bank stated that the individual had some of Plaintiff Angus's personal information but was missing some "key" pieces. On a different occasion, Plaintiff Angus reviewed his bank statement and saw a $5.00 unauthorized charge.

170. As a result of learning of the Data Breach, Plaintiff 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, exploring property fraud monitoring options, researching methods to stop scam calls, responding to attempted and actual fraudulent charges on his accounts, and self-monitoring his financial accounts. This time has been lost forever and cannot be recaptured.

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

172. Plaintiff 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. Plaintiff Angus is particularly concerned that unauthorized individuals will use his Social Security number, name, address, and phone number to purchase a house or open accounts in his name.

173. Plaintiff Angus has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, in combination with his PII being placed in the hands of unauthorized third parties and possibly criminals.

174. Plaintiff 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.

**B. Plaintiff Mark Wiedder**

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

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

177. On or about March 5, 2021, Plaintiff Wiedder learned of the Data Breach via an email from Defendant, sent by "flagstar.advertising@flagstar.com." The email did not disclose that Plaintiff Wiedder's information had been compromised. On or about March 15, 2021, Plaintiff Wiedder received Defendant's *Notice of Data Breach* letter that informed Plaintiff Wiedder that his Social Security number, first name, and last name had been "removed" from the FTA platform by unauthorized actors during the Data Breach.

178. Flagstar has not explained why document(s) containing Plaintiff Wiedder's PII were being stored or shared on the FTA platform.

179. Although Flagstar told Plaintiff Wiedder that "one or more of the documents removed from the Accellion platform" contained his PII, Flagstar has not disclosed to Plaintiff Wiedder what those document(s) are, nor has Flagstar explained whether those document(s) contained other information regarding Plaintiff Wiedder besides the "data elements" Flagstar listed in the notice letter.

180. As a result of the breach, Plaintiff Wiedder signed up for the credit monitoring service provided by Kroll.

181. On or about March 18, 2021, Mr. Wiedder discovered an unauthorized charge of $96.00 on his checking account. In response to the fraudulent charge, Mr. Wiedder spent time contacting his bank and filling out paperwork with the local police to get the charge removed from his account.

182. Following the breach, Plaintiff Wiedder and his spouse have experienced an increase in the volume of suspicious phishing and scam calls and text messages they receive.

183. As a result of the Data Breach, Plaintiff Wiedder has 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, including monitoring identity theft protection services from Kroll and Experian, and filing an identity theft affidavit with a government agency. This time has been lost forever and cannot be recaptured.

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

185. Plaintiff 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.

186. Plaintiff 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 being placed in the hands of unauthorized third parties and possibly criminals.

187. Plaintiff 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.

**C. Plaintiff Tania Garcia**

188. Plaintiff Tania Garcia is a citizen of New Jersey residing in Jamesburg, New Jersey.

189. In 2016, Plaintiff Garcia obtained a residential mortgage loan from Defendant. Plaintiff Garcia's last loan payment to Defendant was in or around 2018, when Plaintiff began making loan payments to a different entity.

190. In connection with her loan application and setting up online bill-pay, Plaintiff Garcia provided financial and other highly sensitive information to Defendant, including her Social Security number, phone number, email address, and bank account information. Plaintiff Garcia reasonably believes her PII was obtained

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

191. Since the Data Breach, Plaintiff Garcia has experienced an increase in the volume of suspicious phishing and scam emails and calls she receives, including emails claiming that unauthorized actors have tried to log into her accounts. As a result, Plaintiff Garcia has been forced to change her phone number multiple times.

192. Since February 1, 2021, Plaintiff Garcia has received multiple notifications from Apple that unauthorized users were attempting to sign in to her Apple account, which is tied to her email address. Plaintiff Garcia spent time addressing these attempted logins, including contacting Apple to unlock her Apple account.

193. After the Data Breach, Plaintiff Garcia's bank notified her of two small fraudulent charges on her bank account. Plaintiff Garcia spent time dealing with the consequences of these charges, including calling the bank to dispute them and receive a refund.

194. Since the Data Breach, Plaintiff Garcia has received notices from Experian that her email address is on the dark web.

195. As a result of learning of the Data Breach, Plaintiff Garcia 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, daily checking her Credit Karma and Experian accounts, and self-monitoring her financial accounts.

196. Plaintiff Garcia suffered actual injury in the form of damages to and loss in market value of her PII—a form of intangible property that Plaintiff Garcia entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

197. Plaintiff Garcia suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

198. Plaintiff Garcia has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

199. Plaintiff Garcia has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**D. Plaintiff Edward Burdick**

200. Plaintiff Edward Burdick is a citizen of Indiana residing in Angola, Indiana.

201. In June 2018, Plaintiff Burdick obtained a residential mortgage loan from Defendant. In connection with his loan application, Plaintiff Burdick provided financial and other highly sensitive information to Defendant, including his Social Security number.

202. On or around March 15, 2021, Plaintiff Burdick learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Plaintiff Burdick on or around that date.[128] The letter confirmed that Plaintiff Burdick's Social Security number, first name, last name, account number, and address had been "removed" from the FTA platform by unauthorized actors during the Data Breach.

203. As a result of learning of the Data Breach and the subsequent fraudulent charges, Plaintiff Burdick 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, 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.

[128] Exhibit 4 (*Notice of Data Breach* sent to Plaintiff Burdick).

204. Plaintiff Burdick suffered actual injury in the form of damages to and loss in market value of his PII—a form of intangible property that Plaintiff Burdick entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

205. Plaintiff Burdick 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.

206. Plaintiff Burdick 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 being placed in the hands of unauthorized third parties and possibly criminals.

207. Plaintiff Burdick 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.

**E. Plaintiff Ray Harter**

208. Plaintiff Ray Harter is a citizen of Missouri residing in St. Louis, Missouri.

209. In or before 2000, Plaintiff Harter obtained a residential mortgage loan from Defendant. In connection with his loan application, Plaintiff Harter provided

financial and other highly sensitive information to Defendant, including his Social Security Number.

210. Plaintiff Harter's last loan payment to Defendant was in or around 2001, when Mr. Harter began making loan payments to a different entity. Plaintiff Harter paid off his mortgage loan in 2019. The Data Breach occurred almost twenty years after the customer relationship with Defendant ended, and more than one year after Plaintiff Harter paid off his mortgage loan.

211. On or around March 15, 2021, Plaintiff Harter learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Plaintiff Harter on or around that date.

212. Plaintiff Harter suffered actual injury in the form of damages to and loss in market value of his PII—a form of intangible property that Plaintiff Harter entrusted to Defendant as an acquired customer, which was compromised in and as a result of the Data Breach.

213. Plaintiff Harter 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.

214. Plaintiff Harter 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 being placed in the hands of unauthorized third parties and possibly criminals.

215. Plaintiff Harter 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.

**F. Plaintiff Danielle Meis**

216. Plaintiff Danielle Meis is a citizen of Nevada residing in Las Vegas, Nevada.

217. In June 2016, Plaintiff Meis, then a resident of Victorville, California, obtained a residential mortgage loan from Defendant. In connection with her loan application, Plaintiff Meis provided financial and other highly sensitive information to Defendant, including her Social Security number, email address, and phone number.

218. As of November 2019, Plaintiff Meis was no longer a Flagstar customer.

219. On or around March 15, 2021, Plaintiff Meis learned of the Data Breach via the *Notice of Data Breach* letter that Defendant sent to Plaintiff Meis on or around that date. In the letter, Defendant informed Plaintiff Meis that document(s) containing her Social Security number, first name, last name, account number, phone

number, and address were "removed" from the FTA platform by unauthorized actors during the Data Breach.

220. Flagstar has not explained why document(s) containing Plaintiff Meis's PII were stored on the FTA platform more than a year after her relationship with Flagstar terminated.

221. Although Flagstar told Plaintiff Meis that "one or more of the documents removed from the Accellion platform" contained her PII, Flagstar has not disclosed to Plaintiff Meis what those document(s) are, nor has Flagstar explained whether those documents contained other information regarding Plaintiff Meis besides the discrete "data elements" Flagstar listed in the notice letter.

222. A few weeks before Plaintiff Meis received the notice letter from Flagstar in mid-March 2021, Plaintiff Meis was notified that an unauthorized user applied for a credit card account in her name. Around that same time, Plaintiff Meis was also notified that an unauthorized user applied for a new phone account in her name. Both instances of fraud appeared on her credit report. Plaintiff Meis spent time responding to these instances of fraud, including contacting the companies involved (Home Depot and T-Mobile) to remove the fraudulent accounts from her credit report. Plaintiff Meis also promptly froze her credit to prohibit further fraud or identity theft.

223. Before being notified of the Data Breach, Plaintiff Meis had intended to purchase a home. Because Plaintiff Meis was forced to freeze her credit, she was unable to obtain a mortgage and purchase a home as intended.

224. Plaintiff Meis has experienced an increase in phishing and scam calls and texts since the Data Breach, including texts alleging that she made large purchases she did not make and prompting her to "dispute" those purchases by clicking on a fraudulent link.

225. As a result of learning of the Data Breach, Plaintiff Meis 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 and self-monitoring her financial accounts. Before the Data Breach, Plaintiff Meis used credit monitoring services through Experian and Equifax. Because of the Data Breach, Plaintiff Meis has continued to use and monitor these services. This time has been lost forever and cannot be recaptured.

226. Plaintiff Meis suffered actual injury in the form of damages to and loss in market value of her PII—a form of intangible property that Plaintiff Meis entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

227. Plaintiff Meis suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

229. Plaintiff Meis has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**G. Plaintiff Jonathan Kelley**

230. Plaintiff Jonathan Kelley is a citizen of Montana residing in Missoula County, Montana.

231. In 2014, Plaintiff Kelley obtained a residential mortgage loan from a different mortgage company. Shortly thereafter, Plaintiff Kelley's mortgage was purchased by Flagstar. In connection with Plaintiff Kelley's loan, Defendant collected financial and other highly sensitive information regarding Plaintiff Kelley, including his Social Security Number.

232. Plaintiff Kelley continued to make loan payments to Defendant until 2024. Despite this ongoing relationship, Defendant stored and/or shared some of

Plaintiff Kelley's most sensitive (and extremely valuable to cyber criminals and identity thieves) PII using the FTA platform, resulting in the exposure of Plaintiff Kelley's PII during the Data Breach.

233. On or around March 29, 2021, Plaintiff Kelley learned of the Data Breach via the *Notice of Data Breach* letter that Defendant sent to Plaintiff Kelley on or around that date. In the letter, Defendant informed Plaintiff Kelley that document(s) containing his Social Security number, first name, last name, phone number, and address were "removed" from the FTA platform by unauthorized actors during the Data Breach.

234. Flagstar has not explained why document(s) containing Plaintiff Kelley's PII were being shared or stored using the FTA platform more than five years after Flagstar began servicing his loan.

235. Although Flagstar told Plaintiff Kelley that "one or more of the documents removed from the Accellion platform" contained his PII, Flagstar has not disclosed to Plaintiff Kelley what those document(s) are, nor has Flagstar explained whether those document(s) contained other information regarding Plaintiff Kelley besides the "data elements" Flagstar listed in the notice letter.

236. Within a few days of receiving the Notice, Plaintiff Kelley called Flagstar to request more information about the breach, and on April 8, 2021, Plaintiff Kelley signed up for the complimentary credit monitoring services offered by

Flagstar through Kroll. Plaintiff Kelley's subscription for credit monitoring expired on April 8, 2023. Flagstar failed to notify Plaintiff Kelley that his subscription was going to expire or had expired. When Plaintiff Kelley asked whether he could re-enroll in the credit monitoring service, Plaintiff Kelley was told he could not re-enroll because the service was "only for companies."

237. As a result of learning of the Data Breach, Plaintiff Kelley 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 and credit reports. This time has been lost forever and cannot be recaptured.

238. Plaintiff Kelley suffered actual injury in the form of damages to and loss in market value of his PII—a form of intangible property that Plaintiff Kelley entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

239. Plaintiff Kelley 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.

240. Plaintiff Kelley has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting

from his PII in combination with his PII being placed in the hands of unauthorized third parties and possibly criminals.

241. Plaintiff Kelley 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.

**H. Plaintiff Ryan Martin**

242. Plaintiff Ryan Martin is a citizen of Pennsylvania residing in East Petersburg, Pennsylvania.

243. Plaintiff Martin refinanced his home in late October/early November 2020. The refinancing company he used forced him to use Defendant as a mortgage provider. In connection with his loan application, Plaintiff Martin provided financial and other highly sensitive information to Defendant, including his Social Security Number.

244. Defendant stored and/or shared some of Plaintiff Martin's most sensitive (and extremely valuable to cyber criminals and identity thieves) PII using Accellion FTA, resulting in the exposure of Plaintiff Martin's PII during the Data Breach.

245. On or around March 15, 2021, Plaintiff Martin learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Plaintiff Martin on or around that date.

246. Since January 2021, Plaintiff Martin has experienced an increase in the volume of "spam" calls he receives. Some of these spam calls are particularly frightening, as the spammers tell Plaintiff Martin personal information about himself as a method of attempting to appear legitimate.

247. In January or February 2021, Santander Bank put a freeze on a credit card owned by Plaintiff Martin and had to issue him a new one. When Plaintiff Martin asked the reason, the bank informed him it was because of a data breach.

248. As a result of learning of the Data Breach, Plaintiff Martin 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. Mr. Martin spends at least double the time monitoring his financial accounts as he did before the Data Breach. This time has been lost forever and cannot be recaptured.

249. Plaintiff Martin suffered actual injury in the form of damages to and loss in market value of his PII—a form of intangible property that Mr. Martin entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

250. Plaintiff Martin 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.

251. Plaintiff Martin 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.

252. Plaintiff Martin 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.

**I. Plaintiff Arthur Dore**

253. Plaintiff Arthur Dore is a citizen of Michigan residing in Detroit, Michigan.

254. On or about September 15, 2020, Plaintiff Dore obtained a residential mortgage loan from Defendant. In connection with his loan application, Plaintiff Dore provided financial and other highly sensitive information to Defendant, including his Social Security number.

255. On or around March 15, 2021, Plaintiff Dore learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Plaintiff Dore on or around that

date.[129] Defendant informed Plaintiff Dore that "one or more of the documents removed from the Accellion platform contained your Social Security Number, Date of Birth, First Name, Address."

256. As a result of learning of the Data Breach, Plaintiff Dore 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 protection options, signing up for credit monitoring, self-monitoring his financial accounts, and spending time contacting his bank to close one checking account. This time has been lost forever and cannot be recaptured.

257. Plaintiff Dore suffered actual injury in the form of damages to and loss in market value of his PII—a form of intangible property that Plaintiff Dore entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

258. Plaintiff Dore 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. These inconveniences have included receiving unsolicited text messages about refinancing his student loans which Plaintiff Dore had not previously received before the breach.

[129] Exhibit 5 (*Notice of Data Breach* sent to Plaintiff Dore).

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

260. Plaintiff Dore 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.

**J. Plaintiff Ann Kelly**

261. Plaintiff Ann Kelly is a citizen of Michigan residing in Allenton, Michigan.

262. In 2010, Plaintiff A. Kelly opened personal financial accounts including a checking account and savings account with the Defendant. In connection with her application, Plaintiff A. Kelly provided financial and other highly sensitive information to Defendant, including her Social Security number.

263. On or around March 15, 2021, Plaintiff A. Kelly learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Plaintiff A. Kelly on or around that date.

264. As a result of learning of the Data Breach, Plaintiff A. Kelly 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 protection options, signing up for credit monitoring, and self-monitoring her financial accounts. This time has been lost forever and cannot be recaptured.

265. Plaintiff A. Kelly suffered actual injury in the form of damages to and loss in market value of her PII—a form of intangible property that Plaintiff A. Kelly entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

266. Plaintiff A. Kelly suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

268. Plaintiff A. Kelly has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**K. Plaintiff Keith Kelly**

269. Plaintiff Keith Kelly is a citizen of Michigan residing in Allenton, Michigan.

270. In 2010, Plaintiff K. Kelly opened personal financial accounts including a checking account and savings account with the Defendant. In connection with his application, Plaintiff K. Kelly provided financial and other highly sensitive information to Defendant, including her Social Security number.

271. On or around March 15, 2021, Plaintiff K. Kelly learned of the Data Breach via the *Notice of Data Breach* that Defendant sent to Plaintiff K. Kelly on or around that date.

272. As a result of learning of the Data Breach, Plaintiff K. Kelly 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 protection options, signing up for credit monitoring, and self-monitoring his financial accounts. This time has been lost forever and cannot be recaptured.

273. Plaintiff K. Kelly suffered actual injury in the form of damages to and loss in market value of her PII—a form of intangible property that Plaintiff K. Kelly entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

274. Plaintiff K. Kelly suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

276. Plaintiff K. Kelly has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

**L. Plaintiff Randy Moniz**

277. Plaintiff Randy Moniz is a citizen of California residing in Livermore, California.

278. Plaintiff Moniz joined Flagstar as an employee in 2017. He provided his PII to Flagstar as a condition of his employment, including his name, Social Security number, email address, date of birth, and other sensitive information.

279. In January 2021, Plaintiff Moniz received an internal email sent to Flagstar employees notifying them that Flagstar had been subject to the cyberattacks. The email did not disclose that Plaintiff Moniz was impacted by the Data Breach.

280. On or around March 15, 2021, Plaintiff Moniz learned that his information was impacted by the Data Breach via the *Notice of Data Breach* letter that Defendant sent Plaintiff Moniz on or around that date. In the letter, Defendant informed Plaintiff Moniz that document(s) containing his Social Security number,

date of birth, first name, and last name were "removed" from the FTA platform by unauthorized actors during the Data Breach.

281. Flagstar has not explained why document(s) containing Plaintiff Moniz's PII were stored on the FTA platform.

282. Although Flagstar told Plaintiff Moniz that "one or more of the documents removed from the Accellion platform" contained his PII, Flagstar has not disclosed to Plaintiff Moniz what those document(s) are, nor has Flagstar disclosed whether those documents contain other information regarding Plaintiff Moniz besides the "data elements" Flagstar listed in the notice letter. Flagstar failed to disclose to Plaintiff Moniz a complete account of his PII that was exfiltrated in the Data Breach. For example, Plaintiff Moniz's home address and email address were also removed from the FTA platform, along with his age, salary, and employee ID number, yet Flagstar failed to disclose to Plaintiff Moniz that these data elements had been breached. Further, Plaintiff Moniz reasonably believes that his personal email address and emergency contact information were also exfiltrated during the Data Breach.

283. After the Data Breach, unauthorized actors accessed Plaintiff Moniz's Walmart account, seemingly using his email address, changed the "delivery address" to an address in New Jersey, and fraudulently charged $44.36 to the account for an

item to be delivered to the changed address. Plaintiff Moniz spent time disputing and cancelling this charge.

284. After the Data Breach, unauthorized actors used Plaintiff Moniz's PII to purchase an IPad Pro for $1,600 at AT&T. Plaintiff Moniz spent time disputing these charges and received confirmation from AT&T's Global Fraud Department in October 2021 that the charges were unauthorized. Plaintiff Moniz also received emails from Paypal reflecting "invoices" requesting payment for items or services he never purchased. In response, Plaintiff Moniz set up 2-step verification for his Paypal account.

285. After the Data Breach, Plaintiff Moniz was notified that unauthorized actors had attempted to log in to Plaintiff Moniz's AOL and Coinbase accounts using his email address. In one instance, Plaintiff Moniz received a call from someone pretending to be a representative of AOL who requested personal information. Plaintiff Moniz hung up and called AOL customer service, who confirmed that they did not contact him. That same day, he received a call from someone pretending to be associated with Coinbase who was trying to access his account. After setting up two-set verification for his AOL account, Plaintiff Moniz has received several email notifications from AOL of log-in attempts from unauthorized users, including in Uruguay, India, Kentucky, Florida, Brazil, New York, Malaysia, Minnesota,

Utah, United Kingdom, Serbia, Mexico, Georgia (US), Barbados, New Jersey, Texas, and Romania.

286. After the Data Breach, Plaintiff Moniz has received numerous alerts that his personal information and email login credentials are on the dark web.

287. As a result of the Data Breach, Plaintiff Moniz has spent time dealing with the consequences of the Data Breach, including changing several of his credit card accounts, updating his automatic billing instructions for most of his accounts, spending between 15-30 hours communicating with banks, setting up two-step authentication and facial ID for many of his accounts, and changing the email address for his financial accounts.

288. Since the Data Breach, Plaintiff Moniz also has experienced an increase in phishing and scam telephone calls.

289. As a result of the Data Breach, Plaintiff Moniz put a freeze on his credit file with the major credit bureaus.

290. Prior to the Data Breach, Plaintiff Moniz purchased a subscription to IDShield for approximately $30.00 a month. Plaintiff Moniz intended to cancel his subscription to IDShield but renewed his subscription because of the Data Breach.

291. Plaintiff Moniz received notice from LegalShield Credit Monitoring that it had discovered his information on the dark web.

292. The exposure of his private and confidential information in the Data Breach has caused Plaintiff Moniz to suffer anxiety related to his personal information being compromised and to devote significantly more time to checking his credit reports and financial accounts for fraudulent activity.

293. Plaintiff Moniz suffered actual injury in the form of damages to and loss in market value of his PII—a form of intangible property that Plaintiff Moniz entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

294. Plaintiff Moniz suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

295. Plaintiff Moniz has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII in combination with his name being placed in the hands of unauthorized third parties and possibly criminals.

296. Plaintiff Moniz 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.

**M. Plaintiff Holly Ringling**

297. Plaintiff Holly Ringling is a citizen of Texas residing in San Antonio,

Texas.

298. Plaintiff Ringling received banking services from Flagstar and provided her PII to receive those services.

299. In approximately March 2021, Plaintiff Ringling believes she received a letter from Flagstar informing her of the Data Breach and advising her to take protective measures. Upon information and belief, her Social Security number, email address, date of birth, and bank account and routing number were taken by unauthorized actors in the Data Breach.

300. In response to the Data Breach, Plaintiff Ringling purchased a subscription for credit monitoring services from Experian for $24 a month and locked her credit file. In response to the Data Breach, Plaintiff Ringling also purchased a subscription for credit monitoring services from Lexington Law for $24.99 a month.

301. After the Data Breach, Plaintiff Ringling experienced multiple fraudulent charges to her accounts. For example, after the data breach, unauthorized actors used funds from her bank account to purchase a $6.50 drink on a Southwest Airlines flight. Further, after the Data Breach, unauthorized actors accessed Plaintiff Ringling's iCloud account, which is tied to Plaintiff Ringling's email address and contained her credit card information, and fraudulently charged $1,600 for a Lowes washer and dryer to her credit card. Plaintiff Ringling spent time dealing with the

consequences of these fraudulent charges, including filling out a police report, locking her credit card, and working with her banks to receive reimbursement.

302. After the Data Breach, unauthorized actors attempted to log in to her TurboTax account in an apparent attempt to file a false tax return. Plaintiff Ringling spent time responding to this unauthorized attempt, including notifying TurboTax of the unauthorized log-in attempt.

303. Since the Data Breach, Plaintiff Ringling has experienced an increase in scam and phishing telephone calls. Plaintiff Ringling has had to block at least 28 phone numbers used by scammers to contact her.

304. Plaintiff Ringling expended additional time dealing with the consequences of the Data Breach, including by re-setting automatic billing instructions tied to her accounts, replacing her debit cards every six months, and daily monitoring her accounts for unauthorized activity.

305. After the Data Breach, Plaintiff Ringling received notice that her personal information had been discovered on the dark web.

306. The exposure of her private, confidential information in the Data Breach has caused Plaintiff Ringling to suffer anxiety related to her personal information being compromised and to devote significantly more time to checking her credit reports and financial accounts for fraudulent activity.

307. Plaintiff Ringling suffered actual injury in the form of damages to and loss in market value of her PII—a form of intangible property that Plaintiff Ringling entrusted to Defendant as a customer, which was compromised in and as a result of the Data Breach.

308. Plaintiff Ringling suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

309. Plaintiff Ringling has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII in combination with her name being placed in the hands of unauthorized third parties.

310. Plaintiff Ringling has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

## CLASS ACTION ALLEGATIONS

311. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

> All individuals residing in the United States whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021.

312. The Florida Subclass that Plaintiff Angus seeks to represent is defined as follows:

> All individuals residing in Florida whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "Florida Subclass").

313. The New Jersey Subclass that Plaintiff Garcia seeks to represent is defined as follows:

> All individuals residing in New Jersey whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "New Jersey Subclass").

314. The Indiana Subclass that Plaintiff Burdick seeks to represent is defined as follows:

> All individuals residing in Indiana whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "Indiana Subclass").

315. The Pennsylvania Subclass that Plaintiff Martin seeks to represent is defined as follows:

> All individuals residing in Pennsylvania whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "Pennsylvania Subclass").

316. The California Subclass that Plaintiffs Wiedder, Meis, and Moniz seek

to represent is defined as follows:

> All individuals residing in California whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "California Subclass").

317. The Michigan Subclass that Plaintiffs Dore, A. Kelly, and K. Kelly seek to represent is defined as follows:

> All individuals residing in Michigan whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "Michigan Subclass").

318. The Borrowers Subclass that Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore seek to represent is defined as follows:

> All individuals residing in the United States who borrowed money from Defendant, including through a mortgage or home equity loan, and whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "Borrowers Subclass").

319. The Banking Subclass that Plaintiffs A. Kelly and K. Kelly seek to represent is defined as follows:

> All individuals residing in the United States who had a checking, savings, or other bank account with Defendant and whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29,

2021 (the "Banking Subclass").

320. The Employee Subclass that Plaintiff Moniz seeks to represent is defined as follows:

> All individuals residing in the United States who were employed by Defendant and whose PII was accessed during the security incident referenced in the Notice of Data Breach that Defendant sent to Plaintiffs and others on or around March 15-29, 2021 (the "Employee Subclass").

321. Excluded from the Classes and Subclasses 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.

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

323. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class and Subclasses are 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.

324. Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class and Subclasses 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 failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices

by failing to safeguard the PII of Plaintiffs and Class Members;

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

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

k. 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.

325. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' 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.

326. 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.

327. Conduct Generally Applicable to the Class, Fed. R. Civ. P. 23(b)(2): 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.

328. Superiority, 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.

329. 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.

330. Defendant's uniform conduct, the identical provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there will be no significant manageability problems with prosecuting this lawsuit as a class action.

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

332. Unless a class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members and may continue to act

unlawfully as set forth in this Complaint.

333. Particular issues under Rule 23(c)(4) may also be 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, consequential, statutory, and/or nominal damages and/or injunctive relief as a result of Defendant's wrongful conduct.

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

334. Plaintiffs repeat and reallege the above allegations as if fully set forth herein.

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

336. 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.

337. 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.

338. 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.

339. 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.

340. 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.

341. 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.

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

343. By undertaking the duty to maintain and secure this data, Defendant had a duty of care to use reasonable means to secure and safeguard its systems and networks—and Plaintiffs and Class members' PII held or transferred within it—to prevent disclosure of the information, and to safeguard the information from cyber theft.

344. Defendant also was in a special relationship with Plaintiffs and Class Members with respect to the hacked information because the end and aim of Defendant's data security measures was to benefit Plaintiffs and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that their systems were sufficiently secure to protect Plaintiffs' and Class Members' personal and medical information.

345. While this special relationship exists independent from any contract, it is recognized by Flagstar's Privacy Policy, as well as applicable laws and regulations. Specifically, Flagstar actively solicited PII as part of its business.

Defendant was solely responsible for and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class members from a resulting data breach.

346. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. It was foreseeable that Plaintiffs and Class members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

347. The policy of preventing future harm further disfavors application of the economic loss rule, particularly given the sensitivity of the private information entrusted to Defendant. A high degree of opprobrium attaches to Defendant's failure to secure Plaintiffs' and Class Members' personal and extremely confidential facts. Defendant had an independent duty in tort to protect this information and thereby avoid reasonably foreseeable harm to Plaintiffs and Class Members.

348. 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.

349. 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.

350. 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.

351. Plaintiffs and the Nationwide Class had no ability to protect their PII that was and may remain in Defendant's possession.

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

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

354. 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.

355. 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.

356. 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.

357. 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.

358. 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.

359. 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.

360. 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.

361. 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.

362. As a result of Defendant's negligence, Plaintiffs and Class members have suffered damages that have included or may, in the future, include, without limitation: (1) loss of the opportunity to control how their personal information is used; (2) loss in the market value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (3) the compromise and theft of their personal information; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and unauthorized use of financial accounts; (5) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports, and assets; (6) unauthorized use of compromised personal information to open new financial and other accounts; (7) continued risk to their personal information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures

to protect the personal information in its possession; (8) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach, and damages for the cost of identity theft protection services for the remainder of their lifetimes.

363. 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.

364. 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.

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

366. 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.

367. 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 Accellion FTA, (b) failing to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on Accellion FTA 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 Accellion and Accellion FTA and (ii) require Accellion 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.

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

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

370. 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 Plaintiffs 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.

371. 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.

372. 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.

373. 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.

374. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

**COUNT II**
**Breach of Implied Contract**
**(On Behalf of Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass)**

375. Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass repeat and reallege the above allegations as if fully set forth herein.

376. When Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass provided their PII to Defendant in exchange for Defendant's financial services and products, they entered into implied contracts with Defendant under which—and by mutual assent of the parties after a meeting of the minds—Defendant agreed to take reasonable steps to protect the PII of Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass.

377. Defendant solicited and invited Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass to provide their PII as part of Defendant's regular business practices and as essential to the financial services and products offered. Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass accepted Defendant's offers by providing their PII to Defendant in connection with the purchase of financial services and products from Defendant.

378. Defendant agreed to protect and safeguard the PII of Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass and prevent it from being disclosed or accessed by unauthorized third parties.

379. Defendant required Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass 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 Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass to provide their dates of birth and financial account information as a condition of being customers of Defendant.

380. As a condition of being customers of Defendant, Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass provided their personal and financial information. In so doing, Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information and to keep such information secure and confidential.

381. Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

382. Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass fully performed their obligations under the implied contracts with Defendant.

383. Defendant breached the implied contracts it made with Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass by failing to safeguard and protect their personal and financial information, including by, among other things:

a. Needlessly storing Plaintiffs' PII for an indefinite period on the FTA platform instead of on Flagstar's allegedly "segmented" network;

b. Failing to clear Plaintiffs' PII from the FTA platform after there was no longer a business justification for keeping it there;

c. Failing to encrypt Plaintiffs' PII on the FTA platform;

d. Failing to password-protect Plaintiffs' PII on the FTA platform.

e. Failing to remove Plaintiffs' PII from the FTA platform after Flagstar knew the FTA platform:

i. Was relegated to "legacy" status and no longer available for licensing by new customers;

ii. Was no longer receiving regular security updates as of February 2019;

iii. Was no longer receiving security scans as of June 2020;

iv. Was no longer operating on a supported operating system as of November 30, 2020;

v. Was under attack by cyber criminals as of December 23, 2020

384. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass 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.

385. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs Angus, Wiedder, Garcia, Burdick, Harter, Meis, Kelley, Martin, and Dore and the Borrowers Subclass are entitled to recover actual, consequential, and nominal damages.

## COUNT III
## Breach of Implied Contract
## (On Behalf of Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass)

386. Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass repeat and reallege the above allegations as if fully set forth herein.

387. When Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass provided their PII to Defendant in exchange for Defendant's financial services and products, they entered into implied contracts with Defendant under which—and by mutual assent of the parties after a meeting of the minds—Defendant agreed to take reasonable steps to protect the PII of Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass.

388. Defendant solicited and invited Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass to provide their PII as part of Defendant's regular business practices and as essential to the financial services and products offered. Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass accepted Defendant's offers by providing their PII to Defendant in connection with the purchase of financial services and products from Defendant.

389. Defendant agreed to protect and safeguard the PII of Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass and prevent it from being disclosed or accessed by unauthorized third parties.

390. Defendant required Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass 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 A. Kelly, K. Kelly, Ringling and the Banking Subclass to provide their dates of birth and financial account information as a condition of being customers of Defendant.

391. As a condition of being customers of Defendant, Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass provided their personal and financial information. In so doing, Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information and to keep such information secure and confidential.

392. Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass value data security and would not have provided their PII to Defendant in the absence of Defendant's implied promise to keep the PII reasonably secure.

393. Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass fully performed their obligations under the implied contracts with Defendant.

394. Defendant breached the implied contracts it made with Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass by failing to safeguard and protect their personal and financial information, including by, among other things:

a. Needlessly storing Plaintiffs' PII for an indefinite period on the FTA platform instead of on Flagstar's allegedly "segmented" network;

b. Failing to clear Plaintiffs' PII from the FTA platform after there was no longer a business justification for keeping it there;

c. Failing to encrypt Plaintiffs' PII on the FTA platform;

d. Failing to password-protect Plaintiffs' PII on the FTA platform.

e. Failing to remove Plaintiffs' PII from the FTA platform after Flagstar knew the FTA platform:

i. Was relegated to "legacy" status and no longer available for licensing by new customers;

ii. Was no longer receiving regular security updates as of February 2019;

iii. Was no longer receiving security scans as of June 2020;

iv. Was no longer operating on a supported operating system as of November 30, 2020;

v. Was under attack by cyber criminals as of December 23, 2020.

395. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass 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.

396. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs A. Kelly, K. Kelly, Ringling and the Banking Subclass are entitled to recover actual, consequential, and nominal damages.

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

397. Plaintiffs and the Nationwide Class repeat and reallege the above allegations as if fully set forth herein.

398. 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.

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

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

401. 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.

402. 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.

403. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiffs and the Nationwide Class is of no legitimate concern to the public.

404. 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' and employees' 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.

405. 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.

406. Defendant acted knowingly and in reckless disregard of Plaintiffs' and Class members' privacy rights because it actually knew that the FTA platform was vulnerable to cyberattack and was being attacked, and that its information security practices were inadequate and insufficient to protect the data stored therein, yet failed to take any action to protect Plaintiffs' PII, including when Defendant knew the FTA platform was under cyberattack in December 2020. Flagstar knew of the need to upgrade to a more secure platform but failed to do so; and likewise failed to implement additional measures like encryption, password-protection, and deletion of unnecessary data, which would have protected Plaintiffs' PII. Defendant knew or should have known that their ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiffs' position.

407. 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.

408. 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.

409. As a direct and proximate result of Defendant's invasion of privacy, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

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

410. Plaintiffs and the Nationwide Class repeat and reallege the above allegations as if fully set forth herein.

411. 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.

412. 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.

413. 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.

414. 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.

415. 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.

416. 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.

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

418. 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.

419. 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.

420. 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.

421. 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.

422. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

## COUNT VI
## Unjust Enrichment
## (On Behalf of Plaintiffs and the Nationwide Class)

423. Plaintiffs and the Nationwide Class repeat and reallege the above allegations as if fully set forth herein.

424. Plaintiffs and the Nationwide Class conferred a monetary benefit on Defendant in the form of monies or fees paid for services from Defendant. Defendant had knowledge of this benefit when it accepted the money from Plaintiffs and the Nationwide Class.

425. The monies or fees paid by Plaintiffs and the Nationwide Class were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiffs and the Nationwide Class.

426. Defendant failed to provide reasonable security, safeguards, and protections to the personal data of Plaintiffs and the Nationwide Class, instead storing and/or sharing the PII of Plaintiffs and the Nationwide Class using the outdated and vulnerable "legacy" Accellion FTA file transfer platform, which resulted in Plaintiffs and the Nationwide Class overpaying Defendant for the services they purchased.

427. Defendant failed to disclose to Plaintiffs and the Nationwide Class that Accellion FTA was inadequate to safeguard the PII of Plaintiffs and the Nationwide Class against theft.

428. Under principles of equity and good conscience, Defendant should not be permitted to retain its ill-gotten gain. Defendant failed to provide adequate safeguards and security measures to protect the PII of Plaintiffs and the Nationwide Class, who paid for such measures but did not receive them.

429. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and the Nationwide Class.

430. Defendant's enrichment at the expense of Plaintiffs and the Nationwide Class is and was unjust.

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

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

432. Plaintiff Angus and the Florida Subclass repeat and reallege the allegations above as if fully set forth herein.

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

434. 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 the PII of Plaintiff Angus and the Florida Subclass;

b. failure to make only authorized disclosures of the PII of Plaintiff Angus and the Florida Subclass; and

c. failure to disclose that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff Angus and the Florida Subclass from theft.

435. 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.

436. 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 the PII of Plaintiff Angus and the Florida Subclass.

437. As a direct and proximate result of Defendant's conduct, Plaintiff Angus and the Florida Subclass have been harmed and have suffered damages including, but not limited to: lost benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

438. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff Angus and the Florida Subclass 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.

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

a. 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;

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

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

d. 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;

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

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

g. 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;

h. 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; and

i. requiring Defendant to thoroughly and regularly evaluate any vendor's or third-party's technology that allows or could allow access to PII and to promptly migrate to superior or more secure alternatives.

## COUNT VIII
## Violation of N.J.S.A. § 56:8-2, The New Jersey Consumer Fraud Act
## (On behalf of Plaintiff Garcia and the New Jersey Subclass)

440. Plaintiff Garcia and the New Jersey Subclass re-allege repeat and reallege the allegations contained above as if fully set forth herein.

441. 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.

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

443. Defendant committed an "unconscionable commercial practice" by failing to use reasonable measures, as interpreted and enforced by the FTC, to protect the PII of Plaintiff Garcia and the New Jersey Subclass.

444. Defendant's acts and practices were unconscionable given the nature and amount of PII it stores and the foreseeable consequences of the far-reaching damage that would inure to Plaintiff Garcia and the New Jersey Subclass by failing to follow reasonable procedures to safeguard their PII.

445. The gravity of the harm to Plaintiff Garcia and the New Jersey Subclass resulting from these unlawful acts and practices outweighed any conceivable reasons, justifications, and/or motives that Defendant 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.*

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

447. 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 Garcia and the New Jersey Subclass, to reasonably rely on those representations and choose Defendant when making a decision about who to entrust their PII to.

448. Defendant's acts and practices as described herein deceived Plaintiff Garcia and the New Jersey Subclass and were highly likely to deceive members of the consuming public. Plaintiff Garcia and the New Jersey Subclass would not have entrusted their PII to Defendant had they been aware that Defendant would unconscionably and unfairly fail to safeguard her PII. Had Plaintiff Garcia and the New Jersey Subclass entrusted their PII to a different bank, their PII would not have been exposed due to Defendant's reckless and intentional acts.

449. Plaintiff Garcia and the New Jersey Subclass have suffered ascertainable loss as a direct result of Defendant's practices described above.

## COUNT IX
## Violation of the Indiana Deceptive Consumer Sales Act, Ind. Code § 24-5-0.5
## (On behalf of Plaintiff Burdick and the Indiana Subclass)

450. Plaintiff Burdick and the Indiana Subclass repeat and reallege the allegations contained above as if fully set forth herein.

451. The Indiana Deceptive Consumer Sales Act ("IDCSA") "shall be liberally construed and applied to promote its purposes and policies," which include "protect[ing] consumers from suppliers who commit deceptive and unconscionable sales acts." Ind. Code § 24-5-0.5-1.

452. The IDCSA defines a "supplier" as "[a] seller, lessor, assignor, or other person who regularly engages in or solicits consumer transactions, including … a manufacturer, wholesaler, or retailer, whether or not the person deals directly with the consumer." *Id.* § 24-5-0.5-2(a)(3)(A).

453. Defendant is a "supplier" under the IDCSA.

454. The IDCSA defines an "incurable deceptive act" as "a deceptive act done by a supplier as part of a scheme, artifice, or device with intent to defraud or mislead." *Id.* § 24-5-0.5-2(a)(8).

455. The IDCSA regulates the conduct of suppliers, as follows:

> A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations.

*Id.* § 24-5-0.5-3(a).

456. Defendant engaged in incurable deceptive acts under the IDCSA related to consumer transactions with Plaintiff Burdick and Indiana Subclass, as follows:

a. Waiting more than 50 days to notify Plaintiff Burdick and the Indiana Subclass of the Data Breach;

b. Failing to have appropriate security safeguards or controls in place to prevent exploitation of vulnerabilities within its system that implicated the security of the PII of Plaintiff Burdick and the Indiana Subclass;

c. Failing to encrypt the sensitive PII of Plaintiff Burdick and the Indiana Subclass, including their Social Security Numbers; and

d. Failing to timely migrate from the "legacy" Accellion FTA file transfer platform to an alternative that would have better secured the PII of Plaintiff Burdick and the Indiana Subclass.

457. The IDCSA provides that "[a] person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater." *Id.* § 24-5-0.5-4(a). Moreover, "[t]he court may increase damages for a willful deceptive act in an amount that does not exceed the greater of: (1) three (3)

times the actual damages of the consumer suffering the loss; or (2) one thousand dollars ($1,000)." *Id.*

458. The IDCSA provides that a senior consumer, defined as "an individual who is at least sixty (60) years of age," may recover treble damages for an incurable deceptive act. *Id.* §§ 24-5-0.5-2(a)(9), 24-5-0.5-4(i).

459. Plaintiff Burdick and the Indiana Subclass are entitled to and demand recovery of the maximum statutory damages available under the IDCSA.

460. Under IDCSA § 24-5-0.5-4(a), Plaintiff Burdick and the Indiana Subclass are entitled to and demand recovery of reasonable attorney fees.

**COUNT X**
**Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law,**
**(73 P.S. §§ 202-1, *et seq.*)**
**(On Behalf of Plaintiff Martin and the Pennsylvania Subclass)**

461. Plaintiff Martin and the Pennsylvania Subclass repeat and reallege the allegations above as if fully set forth herein.

462. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained the PII of Plaintiff Martin and the Pennsylvania Subclass through trade or commerce directly or indirectly affecting Plaintiff Martin and the Pennsylvania Subclass and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

463. 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; and

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

464. 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.

465. 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.

466. As a direct and proximate result of Defendant's conduct, Plaintiff Martin and the Pennsylvania Subclass have been harmed and have suffered damages including, but not limited to: lost benefit of their bargain with Defendant as they

would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; 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.

467. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff Martin and the Pennsylvania Subclass 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.

468. Also as a direct result of Defendant's knowing violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, Plaintiff Martin and the Pennsylvania Subclass are entitled to damages as well as injunctive relief, including, but not limited to:

a. 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;

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

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

d. 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;

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

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

g. 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;

h. 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; and

i. requiring Defendant to thoroughly and regularly evaluate any vendor's or third party's technology that allows or could allow access to PII and to promptly migrate to superior or more secure alternatives.

**COUNT XI**
**Violation of the Michigan Consumer Protection Act,**
**(M.C.L.A. § 445.901 *et seq.*)**
**(On Behalf of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass)**

469. Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass repeat and reallege the allegations contained above as if fully set forth herein.

470. Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass are "persons" as defined by M.C.L.A. § 445.903(d).

471. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by M.C.L.A. § 445.903(g).

472. The MCPA prohibits "[u]nfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce." M.C.L.A. § 445.903(1).

473. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of M.C.L.A. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of M.C.L.A. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of M.C.L.A. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation M.C.L.A. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of M.C.L.A. § 445.903(1)(cc).

474. Defendant's unfair, unconscionable, and deceptive practices include:

e. Failing to implement and maintain reasonable security and privacy measures to protect the PII of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass, which was a direct and proximate cause of the Data Breach;

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

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Rule, Regulation P, and the Safeguards Rule, which was a direct and proximate cause of the Data Breach;

h. Misrepresenting that it would protect the privacy and confidentiality of the PII of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Act, Regulation P, and the Safeguards Rule;

j. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure the PII of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass; and

k. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of the PII of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass, including duties imposed by the FTC Act, the GLBA, the Privacy Act, Regulation P, and the Safeguards Rule.

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

476. Defendant intended to mislead Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass and induce them to rely on its misrepresentations and omissions.

477. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded the rights of Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass.

478. Defendant violated the MCPA by failing to comply with the Michigan Identity Theft Prevention Act (MITPA), which requires Flagstar to give notice of the data breach "without unreasonable delay." M.C.L.A. § 445.72(1), (4). Flagstar

unreasonably delayed in notifying Plaintiffs Dore, A. Kelly, and K. Kelly of the data breach, which prevented Plaintiffs from taking steps to protect their personal information from identity theft and fraud.

479. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant as they would not have paid Defendant for goods and services or would have paid less for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

480. Plaintiffs Dore, A. Kelly, and K. Kelly and the Michigan Subclass seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, restitution, injunctive relief, and any other relief that is just and proper.

**COUNT XII**
**Violation of California's Consumer Privacy Act**
**Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")**
**(On Behalf of Plaintiffs Wiedder, Meis, and Moniz and the California Subclass)**

481. Plaintiffs Wiedder, Meis, and Moniz, on behalf of the California Subclass, repeat and reallege the allegations above as if fully set forth herein.

482. For purposes of this Count, statutory subdivisions invoked are to the CCPA as it existed at the time of the Data Breach, subject to subsequent legislative clarifications.

483. Section 1798.150(a)(1) of the CCPA provides, "[a]ny consumer whose nonencrypted or nonredacted personal information, as defined [by California Civil Code section 1798.81.5(d)(1)(A)] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

484. Plaintiffs Wiedder, Meis, and Moniz and California Subclass members are consumers and California residents as defined by California Civil Code section 1798.140(g).

485. Defendant is a business as defined in California Civil Code section 1798.140. Defendant does business in California, is organized for the profit or financial benefit of its owners, collects PII as defined in California Civil Code section 1798.140, and determines the purposes and means of processing such PII. Further, Defendant has a gross annual revenue of over $25 million and buys, receives, or sells the personal information of at least 50,000 California residents, households, or devices.

486. Defendant collects personal information from, among other sources, consumers who request information from it and consumers who use its services. This PII includes information defined as "sensitive" under the CCPA. Mandiant found that the hackers who perpetrated the Data Breach used "tooling designed to facilitate exfiltration of data from the FTA system."

487. Further, Defendant maintained the PII of California Subclass members' in a form that allowed criminals to access it.

488. Defendant failed to implement a secure system for transferring files. Defendant knew, or should have known, that its network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so that in the event of a data breach

an unauthorized third party cannot read the PII. As a result of Defendant's failure to implement reasonable security procedures and practices, the PII of Plaintiffs and members of the California Subclass was exposed.

489. Defendant consequently violated California Civil Code section 1798.150(a) by failing to prevent the PII of Plaintiffs Wiedder, Meis, and Moniz and California Subclass members from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

490. The PII of Plaintiffs Wiedder, Meis, and Moniz and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's CCPA violations.

491. The PII of Plaintiffs Wiedder, Meis, and Moniz and California Subclass members that was accessed by the cybercriminals in the Data Breach includes nonencrypted and unredacted personal information as set forth in California Civil Code section 1798.81.5(d)(1)(A).

492. Plaintiffs Wiedder, Meis, and Moniz and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

493. Pursuant to Section 1798.150(b) of the CCPA, Plaintiff Moniz gave written notice to Defendant of its violations of section 1798.150(a) by certified mail sent on or before June 19, 2023.

494. Defendant, however, failed to "actually cure" its violations within 30 days of the written notice, and failed to comply with section 1798.150(b) by failing to "provide[] the consumer an express written statement that the violations have been cured and that no further violations shall occur." Nor is any cure reasonably possible, because Plaintiffs Wiedder, Meis, and Moniz and the California Subclass can never regain control of their confidential personal information taken in the Data Breach.

495. Defendant also failed to "actually cure" its violations by, among other things, not encrypting the PII of Plaintiffs Wiedder, Meis, and Moniz and of the California Subclass, and by not deleting the PII of Plaintiffs Wiedder, Meis, and Moniz and of the California Subclass that Defendant no longer had a reasonable need to maintain in an Internet-accessible environment.

496. Plaintiffs Wiedder, Meis, and Moniz and California Subclass members accordingly seek actual and statutory damages under California Civil Code section 1798.150(a)(1)(A), injunctive and declaratory relief, reasonable attorneys' fees and costs pursuant to California Code of Civil Procedure section 1021.5, and any other relief deemed appropriate by the Court, for Defendant's CCPA violations.

## COUNT XIII
## Violation of California's Customer Records Act
## Cal. Civ. Code § 1798.80, *et seq.* ("CCRA")
## (On Behalf of Plaintiffs Wiedder, Meis, and Moniz and the California Subclass)

497. Plaintiffs Wiedder, Meis, and Moniz and the California Subclass repeat and reallege the allegations above as if fully set forth herein.

498. Plaintiffs Wiedder, Meis, and Moniz and California Subclass members are "customers" within the meaning of California Civil Code section 1798.80(c), as they provided personal information to Defendant for the purpose of obtaining services from Defendant.

499. Defendant is a "business" within the meaning of California Civil Code section 1798.80(a).

500. The CCRA provides that "[a] person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California . . . whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person . . . in the most expedient time possible and without unreasonable delay[.]" Cal. Civ. Code § 1798.82.

501. The Data Breach constitutes a breach of security within the meaning of section 1798.82. PII stolen in the Data Breach, such as full names, addresses,

telephone numbers, birthdates, Social Security numbers, and financial information, and as well as other information, constitutes "personal information" within the meaning of section 1798.80(e).

502. In violation of the CCRA, Defendant failed to promptly notify Plaintiffs Wiedder, Meis, and Moniz and California Subclass members of the Data Breach. Timely disclosure was necessary so that Plaintiffs and Class members could, among other things: (1) purchase identity protection, monitoring, and recovery services; (2) flag asset, credit, and tax accounts for fraud, including by reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the IRS; (3) purchase or otherwise obtain credit reports; (4) place or renew fraud alerts on a quarterly basis; (5) intensively monitor loan data and public records; and (6) take other steps to protect themselves and attempt to avoid or recover from identity theft.

503. As a result of Defendant's unreasonable delay in notifying its customers, Plaintiffs Wiedder, Meis, and Moniz and California Subclass members, of the Data Breach, they were deprived of an opportunity to take timely and appropriate self-protective measures, such as requesting a credit freeze. In addition, as a result of the delay, Plaintiffs Wiedder, Meis, and Moniz and California Subclass members have suffered (and will continue to suffer) economic damages and other injuries and actual harm including, without limitation: (1) the compromise and theft of their personal information; (2) loss of the opportunity to control how their

personal information is used; (3) loss of market value and use of their personal information entrusted to Defendant with the understanding that Defendant would safeguard it against theft and not allow it to be accessed and misused by third parties; (4) out-of-pocket costs associated with the prevention and detection of, and recovery from, identity theft and misuse of their personal information; (5) continued undue risk to their personal information; and (6) future costs in the form of time, effort, and money they will expend to prevent, detect, contest, and repair the adverse effects of their personal information being stolen in the Data Breach.

504. Therefore, on behalf of the California Subclass, Plaintiffs Wiedder, Meis, and Moniz seek actual damages under California Civil Code section 1798.84(b), injunctive and declaratory relief, and any other relief deemed appropriate by the Court.

## COUNT XIV
## Violation of California's Unfair Competition Law
## Cal. Bus. & Prof. Code §§ 17200, *et seq.*
## (On Behalf of Plaintiffs Wiedder, Meis, and Moniz and the California Subclass)

505. Plaintiffs Wiedder, Meis, and Moniz and the California Subclass repeat and reallege the allegations above as if fully set forth herein.

506. Flagstar is a "person" as defined by Cal. Bus. & Prof. Code §17201.

507. Flagstar violated Cal. Bus. & Prof. Code §§ 17200, et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

508. Flagstar's "unfair" acts and practices include:

a. Flagstar failed to implement and maintain reasonable security measures to protect Plaintiffs' and the California Subclass Members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach.

b. Flagstar failed to identify foreseeable security risks and remediate identified security risks. following previous cybersecurity incidents, as described herein. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiffs and the California Subclass Members, whose PII has been compromised.

c. Flagstar's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; California's Consumer Records Act, Cal. Civ. Code § 1798.81.5; and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

d. Flagstar's failure to implement and maintain reasonable security measures also resulted in substantial consumer injuries, as described

above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Flagstar's grossly inadequate security, they could not have reasonably avoided the harms that Flagstar caused.

e. Flagstar engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

509. Flagstar has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification); California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq.; the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; and California common law.

510. Flagstar's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and the California Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify and remediate foreseeable security and privacy risks and adequately improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTC Act (15 U.S.C. § 45); and the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and the California Subclass Members' PII; and

g. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and the California Subclass

Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45; the GLBA, its Privacy Rule and/or Regulation P, and its Safeguards Rule; California's Consumer Privacy Act, Cal. Civ. Code § 1798.100; California's Consumer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.* and 1798.81.5, which was a direct and proximate cause of the Data Breach.

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

512. As a direct and proximate result of Flagstar's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and the California Subclass Members were injured and suffered monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Flagstar's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

513. Flagstar acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and the

California Subclass Members' rights. Flagstar's past data breach put it on notice that its security and privacy protections were inadequate.

514. Plaintiffs and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Flagstar's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

## PRAYER FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court enter an Order:

A. certifying the Nationwide Class, the Borrowers Subclass, the Banking Subclass, the California Subclass, the Florida Subclass, the Indiana Subclass, the Michigan Subclass, the New Jersey Subclass, and the Pennsylvania Subclass, and appointing Plaintiffs and their Counsel to represent each such Class and Subclass;

B. 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;

C. providing injunctive or 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 and other means, 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, including vendor risk management assessments, risk-based patch management and threat intelligence services 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 any third-party managed 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 all 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 and alerting;

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 immutable logging and monitoring programs sufficient to track traffic to and from Defendant's systems; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation including the Privacy principle, 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; and

xvii. requiring Defendant to thoroughly and regularly evaluate any vendor's or third party's technology that allows or could allow access to PII, or is deployed as a trusted service with access to any systems that may contain PII, and to promptly migrate to superior or more secure alternatives;

D. For an award of damages, including actual, consequential, statutory, and nominal 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 and post-judgment 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: May 13, 2024

Respectfully submitted,

*/s/ John A. Yanchunis*

John A. Yanchunis (*interim lead counsel*)
**MORGAN & MORGAN COMPLEX LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com

Norman E. Siegel MO #44378
**STUEVE SIEGEL HANSON LLP**
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com

Adam E. Polk (State Bar No. 273000)
Jordan Elias (State Bar No. 228731)
Simon S. Grille (State Bar No. 294914)
**GIRARD SHARP LLP**
601 California Street, Suite 1400
San Francisco, CA 94108
Tel: (415) 981-4800
apolk@girardsharp.com

jelias@girardsharp.com
sgrille@girardsharp.com

Krysta Kauble Pachman (280951)
Michael Gervais (330731)
Steven G. Sklaver (237612)
Kevin R. Downs (331993)
**SUSMAN GODFREY L.L.P.**
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067-6029
Tel: (310) 789-3100
kpachman@susmangodfrey.com
mgervais@susmangodfrey.com
ssklaver@susmangodfrey.com

E. Powell Miller
**The Miller Law Firm, P.C.**
950 W. University Drive, Suite 300
Rochester, Michigan 48307
Telephone: (248) 841-2200
epm@millerlawpc.com

***Executive Committee:***

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, L.P.A
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
Email: jgoldenberg@gs-legal.com

Gary E. Mason*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
Email: gmason@masonllp.com

Charles E. Schaffer*

LEVIN, SEDRAN & BERMAN, LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (212) 592-1500
Email: cschaffer@lfsblaw.com

M. Anderson Berry
**CLAYEO C. ARNOLD,**
**A PROFESSIONAL LAW CORP.**
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com

Brian D. Flick (OH #0081605)
DannLaw
P.O. Box 6031040
Cleveland, Ohio 44103
Phone: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

Bryan L. Bleichner*
Chestnut Cambronne PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
bbleichner@chestnutcambronne.com

* Denotes Applications for Admission pending or to be filed

**CERTIFICATE OF SERVICE**

I, the undersigned, do hereby certify that on May 13, 2024, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

*/s/ John A. Yanchunis*

John A. Yanchunis

# Exhibit 1

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.

# Exhibit 2

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



**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.

# Exhibit 3

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<br>www.fraudalerts.equifax.com<br>P. O. Box 105788<br>Atlanta, GA 30348 | (888) 397-3742<br>www.experian.com/fraud/center<br>P. O. Box 9554<br>Allen, TX 75013 | (800) 680-7289<br>www.transunion.com/personal credit/<br>credit disputes/fraud-alerts.page<br>P. O. Box 6790<br>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<br>www.fraudalerts.equifax.com<br>P. O. Box 105788<br>Atlanta, GA 30348 | (888) 397-3742<br>www.experian.com/fraud/center<br>P. O. Box 9554<br>Allen, TX 75013 | (800) 680-7289<br>www.transunion.com/personal credit/<br>credit disputes/fraud-alerts.page<br>P. O. Box 6790<br>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).

# Exhibit 4

Flagstar Bank

**IMPORTANT INFORMATION**
**PLEASE REVIEW CAREFULLY**

March 15, 2021

Edward L. Burdick
[redacted]

## Notice of Data Breach

Dear Edward L. Burdick,

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, Account 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.

# Exhibit 5

Flagstar Bank

***IMPORTANT INFORMATION***
***PLEASE REVIEW CAREFULLY***

March 15, 2021

Arthur Dore
[redacted]

## Notice of Data Breach

Dear Arthur Dore,

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, Date of Birth, First Name, 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.