

1 Kara M. Wolke (SBN 241521)
kwolke@glancylaw.com

2 Marc L. Godino (SBN 182689)
mgodino@glancylaw.com

3 Jonathan Rotter (SBN 234137)
jrotter@glancylaw.com

4 Pavithra Rajesh (SBN 323055)
prajesh@glancylaw.com

5 GLANCY PRONGAY & MURRAY LLP

6 1925 Century Park East, Suite 2100

7 Los Angeles, California 90067

8 Telephone: (310) 201-9150

9 Facsimile: (310) 201-9160

10 Mary Jane Fait (*pro hac vice* forthcoming)

11 LAW OFFICES OF MARY JANE FAIT, PLLC

12 13820 Emerson Street

13 Palm Beach Gardens, FL 33418

14 Telephone: (847) 922-6729

15 Email: mjf@faitlawoffices.com

16 *Attorneys for Plaintiff Janet Pollard*

17
18 **UNITED STATES DISTRICT COURT**

19 **NORTHERN DISTRICT OF CALIFORNIA**

20 JANET POLLARD, individually and on behalf
21 of all others similarly situated,

22 Plaintiff,

23 v.

24 ACCELLION, INC., and FLAGSTAR
25 BANCORP, INC. d/b/a FLAGSTAR BANK,

26 Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

1 Plaintiff Janet Pollard (“Plaintiff”), individually and on behalf of the class defined herein,
2 alleges the following upon personal knowledge as to facts concerning herself and her actions and
3 upon information and belief, including based on her counsel’s investigation, as to all other matters.

4 **I. SUMMARY OF THE ACTION**

5 1. In December 2020, Accellion’s electronic information systems were compromised,
6 exposing customers’ personally identifiable information (“PII”), including names, Social Security
7 numbers, dates of birth, driver’s license numbers and/or state identification numbers, bank account
8 information, and employment information to third parties.

9 2. Accellion is a cloud computing company that offers a product called “File Transfer
10 Appliance (“FTA”), a physical device that companies use in their server rooms that allows users to
11 share secure, encrypted files that are too large to send via email. Recipients can click a link to files
12 hosted on FTA that can be viewed or downloaded. FTA was first released in May 2005, and by
13 2020, it had become outdated and was on the verge of its “end-of-life.” However, Accellion
14 continued to market and sell FTA.

15 3. On or about December 16, 2020, Accellion learned that unauthorized third parties
16 were able to get control over the FTA device and obtain information, including PII from the devices.
17 On or about January 12, 2021, almost a full month after learning of the breach, Accellion announced
18 that unauthorized individuals had gained access to its legacy file transfer software.

19 4. Plaintiff and other Class members have, and will continue to be injured, by the
20 exposure of their PII. Attackers have been able to decrypt and download all files on the FTA device,
21 and the stolen files are available for purchase on the dark web. This PII can be used to open
22 unauthorized financial accounts in the Class members’ names and obtain government benefits on
23 behalf of Class members.

24 5. Plaintiff and other Class Members will incur significant costs and expenses to
25 counter these actors’ efforts by, for example, obtaining credit monitoring services, credit reports,
26 and other protective measures to deter and detect identity theft.

27 **II. PARTIES**

28 6. Plaintiff Janet Pollard is an adult individual who resides in Missouri.

1 7. Defendant Accellion, Inc. is a Delaware corporation with its principal executive
2 offices located at 1804 Embarcadero Road, Suite 200, Palo Alto, California.

3 8. Defendant Flagstar Bancorp, Inc. d/b/a Flagstar Bank (“Flagstar”) is a Michigan
4 corporation with its principal executive offices located at 5151 Corporate Drive, Troy, Michigan
5 48098. According to its website, Flagstar operates 150 branches in Michigan, Indiana, California,
6 Wisconsin, and Ohio.

7 **III. JURISDICTION AND VENUE**

8 9. This Court has subject matter jurisdiction over this action under the Class Action
9 Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million exclusive of
10 interest and costs. At least one Plaintiff and one Defendant are citizens of different states. There are
11 more than 100 putative Class Members.

12 10. This Court has personal jurisdiction over Defendant because its principal place of
13 business is in this District and Defendant has sufficient contacts in this District.

14 11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because Defendant
15 conducts substantial business in this District and California is the principal place of business for
16 Defendant.

17 **IV. RELATED ACTIONS AND INTRADISTRICT ASSIGNMENT**

18 12. This case arises out of the same core of operative facts as *Brown v. Accellion, Inc.*,
19 No. 5:21-cv-01155-EJD (N.D. Cal.), *Zebelman v. Accellion, Inc.*, No. 5:21-cv-01203-EDJ (N.D.
20 Cal.), *Rodriguez v. Accellion, Inc.*, 5:21-cv-01272-EJD (N.D. Cal.), *Stobbe v. Accellion, Inc.*, 5:21-
21 cv-01353-EJD (N.D. Cal.), *Price v. Accellion, Inc.*, No. 5:21-cv-01430-EJD (N.D. Cal.), *Whittaker*
22 *v. Accellion, Inc.*, No. 5:21-cv-01708-EJD (N.D. Cal.), *Cochran v. Accellion, Inc. et al.*, No. 5:21-
23 cv-01887-EDG (N.D. Cal.), and *Beyer v. Flagstar Bancorp.*, No. 5:21-cv-02239-EJD (N.D. Cal.).

24 13. Assignment to the San Jose Division is appropriate under Local Rule 3-2(c) and (e)
25 because Accellion is headquartered in Palo Alto, California, and a substantial part of the events or
26 omissions which give rise to the claim occurred in Santa Clara County.

27
28

1 **V. FACTUAL ALLEGATIONS**

2 **A. Background**

3 14. Accellion is a cloud computing company that offers products for secure file sharing
4 and collaboration. Its FTA product allows users to send encrypted files that are too large to send as
5 email attachments.

6 15. Accellion purports to offer the secure transfer of sensitive information. Specifically,
7 its website¹ states, in relevant part, that Accellion’s secure file sharing “[g]ive[s] users a simple,
8 secure, private way to share confidential information” and “upload sensitive content in compliance.”

9 16. Accellion also claims to employ an enterprise content firewall that “prevents data
10 breaches and compliance violations from third party cyber risk. . . . When employees click the
11 Accellion button, they know it’s the safe, secure way to share sensitive information with the outside
12 world.”²

13 17. The company further claims that its FTA product “helps worldwide enterprises . . .
14 transfer large and sensitive files securely using a 100% private cloud, on-premises or hosted.”³ More
15 specifically, Accellion states that “in today’s breach-filled, over-regulated world, you need even
16 broader protection and control. Protect all your external file sharing – no matter what the source,
17 device or location – with the industry-leading governance and security of Accellion’s new
18 platform.” *Id.*

19 18. However, Accellion recently conceded that the FTA product is an obsolete “legacy
20 product” that was “nearing end-of-life,”⁴ leaving it vulnerable to attack.

21 19. And, the company has been encouraging users to discontinue their use of FTA.
22 Accellion’s Chief Information Security Officer, Frank Balonis, stated: “Future exploits of [FTA]

23
24 ¹ <https://www.accellion.com/platform/simple/secure-file-sharing/>

25 ² <https://www.accellion.com/company/>

26 ³ <https://www.accellion.com/products/fta/>

27 ⁴ [https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-
28 security-incident/](https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/)

1 . . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the
2 last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain
3 committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon
4 as possible.”⁵ Accellion’s Chief Marketing Officer, Joel York, similarly stated, concerning the FTA
5 product, that “[i]t just wasn’t designed for these types of threats.”⁶

6 **B. The Data Breach**

7 20. In mid-December 2020, Accellion became aware of a “zero-day vulnerability” in its
8 FTA product, i.e. a security flaw known to the software vendor but without a patch to resolve it.⁷ A
9 customer who received an alert from the FTA internal anomaly detector notified Accellion of the
10 details of the alert. Over the next several days, Accellion identified two vulnerabilities that
11 compromised FTA devices: (a) an SQL injection, allowing attackers to obtain any data contained in
12 the FATA internal database and storage devices; and (2) an OS Command Execution, allowing
13 attackers to execute arbitrary actions on the FTA device. Together, these two vulnerabilities enabled
14 attackers to exploit and obtain PII from FTA devices, seizing data from up to 300 of the company’s
15 clients, including corporations, law firms, banks, universities, and other entities.

16 21. One article⁸ described the method of attack:

17 The adversary exploited [the FTA’s] vulnerabilities to install a hitherto unseen Web
18 shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data
19 from victim networks. Mandiant’s telemetry shows that DEWMODE is designed to
20 extract a list of available files and associated metadata from a MySQL database on
21 Accellion’s FTA and then download files from that list via the Web shell. Once the
22 downloads complete, the attackers then execute a clean-up routine to erase traces of
23 their activity.

23 ⁵ <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/>

24 ⁶ <https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/>

26 ⁷ <https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident>

28 ⁸ <https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226>

1 22. Though Accellion released patches on December 20 and December 24, 2020, the
2 company did not publish patch notes for the firmware update or immediately assign CVE security
3 bug identifiers to the vulnerabilities, which is the standard practice for data breaches to ensure timely
4 dissemination of information. As a result, there was a delay in applying the patch by several system
5 administrators, providing additional time for the attackers to exploit the vulnerabilities.

6 23. On January 12, 2021, Accellion announced that it had resolved a vulnerability and
7 “released a patch within 72 hours to the less than 50 customers affected.”

8 24. The attacks continued from at least mid-December 2020 and into January 2021 as
9 the attackers continued to exploit vulnerabilities in the FTA platform. Armed with the sensitive data,
10 the criminals began to extort Accellion’s clients, warning that the stolen information would be made
11 public unless ransom was paid.⁹ In several instances, these attackers followed through on their
12 threats and published the PII online. For example, the attackers sent the following email:

13 Hello!

14 Your network has been hacked, a lot of valuable data stolen. <description of stolen data,
15 including the total size of the compressed files> We are the CLOP ransomware team, you can
16 google news and articles about us. We have a website where we publish news and stolen files
17 from companies that have refused to cooperate. Here is his address [http://\[redacted\].onion/](http://[redacted].onion/)
18 - use TOR browser or [http://\[redacted\].onion.dog/](http://[redacted].onion.dog/) - mirror. We are visited by 20-30 thousand
19 journalists, IT experts, hackers and competitors every day. We suggest that you contact us via
20 chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use
21 TOR browser We don't want to hurt, our goal is money. We are also ready to provide any
22 evidence of the presence of files with us.

23 **C. Plaintiff’s Damages**

24 25. Flagstar is one of the largest bank mortgage originators nationally and the second
25 largest savings bank in the country. According to its website, Flagstar “operate[s] 150 branches in
26 Michigan, Indiana, California, Wisconsin, and Ohio and provide[s] a full complement of products
27 and services for consumers and businesses.”¹⁰ Its “mortgage division operates nationally through
28

⁹ <https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/>

¹⁰ <https://www.flagstar.com/about-flagstar.html>

1 103 retail locations and a wholesale network of approximately 2,350 third-party mortgage
2 originators.”

3 26. On March 5, 2021, Flagstar confirmed that the PII of certain customers was
4 compromised in the data breach of its file transfer software vendor, Accellion. According to
5 Flagstar’s statement, Accellion “informed Flagstar on January 22, 2021.” A statement on the
6 company’s website stated:

7 **What Happened?**

8 Accellion, a vendor that Flagstar uses for its file sharing platform, informed Flagstar
9 on January 22, 2021, that the platform had a vulnerability that was exploited by an
10 unauthorized party. After Accellion informed us of the incident, Flagstar
11 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.

12 Upon discovery, we acted immediately to contain the threat and engaged a team of
13 third-party forensic experts to investigate and determine the full scope of this
14 incident. After a thorough, diligent review of the data, we are now in the process of
notifying impacted customers directly via U.S. Mail.

15 Flagstar has been and remains fully operational, and other parts of our IT
16 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.

17 27. Plaintiff received a letter dated March 15, 2021 from Flagstar informing her of the
18 breach. In addition to general information about the breach, it stated:

19 **What Information Was Involved?**

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

22 28. Flagstar’s letter to Plaintiff further stated that, “[o]ut of an abundance of caution we
23 have secured the services of Kroll to provide identity monitoring at no cost to you for two years. . . .
24 Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft
25 Restoration.”

26 29. In the wake of the breach, Plaintiff has experienced fraudulent credit card charges.
27
28

1 **VI. CLASS ACTION ALLEGATIONS**

2 30. Plaintiff brings this action on behalf of herself and all others similarly situated
3 pursuant to Federal Rules of Civil Procedure, Rule 23(a), 23(b)(2) and 23(b)(3). Plaintiff brings this
4 action on behalf of a Class, defined as:

5 All residents of the United States whose PII was compromised in the data breach
6 involving Accellion's FTA product that occurred throughout December 2020 and
7 January 2021.

8 Plaintiff also brings this action on behalf of a Missouri subclass, defined as:

9 All residents of Missouri whose PII was compromised in the data breach involving
10 Accellion's FTA product that occurred throughout December 2020 and January
11 2021.

12 Plaintiff also brings this action on behalf of a subclass of Flagstar customers, defined
13 as:

14 All individuals whose PII was entrusted to Flagstar and was compromised in the data
15 breach of Flagstar's operations via Accellion's FTA product that occurred between
16 December 2020 and January 2021.

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

24 32. Plaintiff reserves the right to modify or amend the definition of the proposed class
25 before the Court determines whether certification is appropriate.

26 33. This action has been brought and may properly be maintained as a class action under
27 Federal Rules of Civil Procedure, Rule 23, because there is a well-defined community of interest in
28 the litigation, the proposed class is easily ascertainable, and Plaintiff is a proper representative of
the Class.

34. **Numerosity.** The members of the Class are so numerous that joinder of all of them
is impracticable.

1 35. **Commonality.** There are questions of law and fact common to the Class, which
2 predominate over any questions affecting only individual Class Members. These common questions
3 of law and fact include, without limitation:

4 (a) Whether Defendants engaged in the conduct alleged herein;

5 (b) Whether Defendants had a legal duty to adequately protect Plaintiff's and Class
6 members' personal information;

7 (c) Whether Defendants breached their legal duty by failing to adequately protect
8 Plaintiff's and Class members' personal information;

9 (d) Whether Defendants failed to implement and maintain reasonable security measures
10 appropriate to the nature and scope of the information compromised in the data
11 breach;

12 (e) Whether Defendants violated privacy rights of Plaintiff and Class members;

13 (f) Whether Plaintiff and Class members are entitled to recover actual damages and/or
14 statutory damages; and

15 (g) Whether Plaintiff and class members are entitled to equitable relief, including
16 injunctive relief, restitution, disgorgement, and/or the establishment of a constructive
17 trust.

18 36. **Typicality.** Plaintiff's claims are typical of those of other Class members because
19 Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

20 37. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and
21 protect the interests of the Class members. Plaintiff's counsel are competent and experienced in
22 litigating class actions.

23 38. **Predominance.** Defendants have engaged in a common course of conduct toward
24 Plaintiff and Class members in that Plaintiff's and Class members' PII was exposed via Accellion's
25 FTA product and unlawfully accessed in the same way. The common issues set forth herein arising
26 from Defendants' conduct predominate over any individualized issues. Adjudication of these
27 common issues in a single action has important and desirable advantages of judicial economy.
28

1 48. Defendants breached these duties by the conduct alleged herein, including: (a) failing
2 to protect the PII; (b) failing to maintain adequate data security practices to safeguard the PII; and
3 (c) failing to disclose the material fact that Defendant’s data security practices were inadequate to
4 safeguard the PII.

5 49. The conduct alleged herein caused Plaintiff and Class members to be exposed to
6 fraud and be harmed as detailed herein. Plaintiff and Class members were foreseeable victims of
7 Defendants’ inadequate data security practices and in fact suffered damages caused by Defendants’
8 breaches of their duties.

9 50. Defendants knew of the serious harms that could result through the wrongful
10 disclosure of the PII of Plaintiffs and the Class.

11 51. Defendants’ failure to comply with industry standards further demonstrates their
12 negligence in failing to exercise reasonable care in safeguarding and protecting the PII of Plaintiff
13 and the Class.

14 52. But for Defendants’ wrongful and negligent breach of its duties owed to Plaintiff and
15 the Class, their PII would not have been compromised. Defendants’ negligence was a direct and
16 legal cause of the exposure of Plaintiff’s and the Class members’ PII and all resulting damages.

17 53. The injury and harm suffered by Plaintiff and the Class were a reasonably foreseeable
18 result of Defendants’ failure to cure those numerous vulnerabilities or, at a minimum, exercise
19 reasonable care in safeguarding and protecting the PII of Plaintiff and the other Class members.

20 54. As a result of Defendants’ misconduct, the PII of Plaintiff and the Class was
21 compromised and their PII was disclosed to third parties without their consent, placing them at a
22 greater risk of identity theft. Plaintiff and the Class have also suffered out-of-pocket losses related
23 to identity theft losses or protective measures.

24 55. Defendants’ misconduct alleged herein was carried out with a willful and conscious
25 disregard of the rights or safety of Plaintiff and the Class and subjected them to unjust hardship in
26 conscious disregard of their rights.

27 56. Plaintiff, on behalf of herself and all other Class Members, requests the relief
28 described below.

SECOND CAUSE OF ACTION

(Negligence Per Se)

1
2
3 57. Plaintiff realleges and incorporates by reference each and every allegation set forth
4 above.

5 58. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Accellion had a
6 duty to provide adequate data security practices, including in connection with its sale of its FTA
7 platform, to safeguard Plaintiff’s and Class members’ PII.

8 59. Accellion breached its duties to Plaintiff and Class members under the Federal Trade
9 Commission Act (15 U.S.C. § 45) and Flagstar breached its duties to Plaintiff and Class members
10 under the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*), among other laws, by failing to
11 provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA
12 platform in order to safeguard Plaintiff’s and Class members’ PII.

13 60. Defendants’ failure to comply with applicable laws and regulations constitutes
14 negligence per se.

15 61. But for Defendants’ wrongful and negligent breach of its duties owed to Plaintiff and
16 Class members, Plaintiff and Class members would not have been injured.

17 62. The injury and harm suffered by Plaintiff and Class members was the reasonably
18 foreseeable result of Defendants’ breaches of their duties. Defendants knew or should have known
19 that they were failing to meet its duties and that their breaches would cause Plaintiff and Class
20 members to experience the foreseeable harm associated with the exposure of its PII.

21 63. As a direct and proximate result of Defendants’ negligent conduct, Plaintiff and Class
22 members now face an increased risk of future harm. As a direct and proximate result of Defendants’
23 negligent conduct, Plaintiff and Class members have suffered injury and are entitled to damages in
24 an amount to be proven at trial.

25 **THIRD CAUSE OF ACTION**

26 **(Invasion of Privacy)**

27 64. Plaintiff and Class members reallege and incorporate by reference each and every
28 allegation set forth above.

1 65. Plaintiff and Class members had a legitimate expectation of privacy to their PII and
2 were entitled to the protection of this information against disclosure to unauthorized third parties.

3 66. Defendants owed a duty to Plaintiff and Class members to keep their PII contained
4 as a part thereof, confidential.

5 67. Defendants failed to protect and released to unknown and unauthorized third parties
6 the PII of Plaintiff and Class members.

7 68. Defendants allowed unauthorized and unknown third parties access to and
8 examination of the PII of Plaintiff and Class members, by way of Defendant's failure to protect the
9 PII.

10 69. The unauthorized release to, custody of, and examination by unauthorized third
11 parties of the PII of Plaintiff and Class members is highly offensive to a reasonable person.

12 70. The intrusion was into a place or thing, which was private and is entitled to be private.
13 Plaintiff and Class members disclosed their PII to Defendants in connection with services obtained
14 from Accellion and/or Flagstar, but privately with an intention that the PII would be kept
15 confidential and would be protected from unauthorized disclosure. Plaintiff and Class members were
16 reasonable in their belief that such information would be kept private and would not be disclosed
17 without their authorization.

18 71. The data breach constitutes an intentional interference with Plaintiff's and Class
19 members' interest in solitude or seclusion, either as to their persons or as to their private affairs or
20 concerns, of a kind that would be highly offensive to a reasonable person.

21 72. Defendants acted with a knowing state of mind when it permitted the data breach to
22 occur because it was with actual knowledge that their information security practices were inadequate
23 and insufficient.

24 73. Because Defendants acted with this knowing state of mind, they had notice and knew
25 the inadequate and insufficient information security practices would cause injury and harm to
26 Plaintiff and Class members.

27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

DATED: April 8, 2021

GLANCY PRONGAY & MURRAY LLP

By: /s/ Jonathan Rotter

Kara M. Wolke

Marc L. Godino

Jonathan Rotter

Pavithra Rajesh

1925 Century Park East, Suite 2100

Los Angeles, California 90067

Telephone: (310) 201-9150

Facsimile: (310) 201-9160

Email: info@glancylaw.com

Mary Jane Fait (*pro hac vice* forthcoming)

LAW OFFICES OF MARY JANE FAIT, PLLC

13820 Emerson Street

Palm Beach Gardens, FL 33418

Telephone: (847) 922-6729

Email: mjf@faitlawoffices.com

Attorneys for Plaintiff Janet Pollard