

1 M. ANDERSON BERRY (262879)
2 GREGORY HAROUTUNIAN (330263)
3 **CLAYEO C. ARNOLD,**
4 **A PROFESSIONAL LAW CORP.**
5 865 Howe Avenue
6 Sacramento, CA 95825
7 Telephone: (916) 239-4778
8 Facsimile: (916) 924-1829
9 *aberry@justice4you.com*
10 *gharoutunian@justice4you.com*

11 TERENCE R. COATES (*pro hac vice* forthcoming)
12 **MARKOVITS, STOCK & DEMARCO, LLC**
13 3825 Edwards Road, Suite 650
14 Cincinnati, OH 45209
15 Phone: (513) 665-0204
16 Fax: (513) 665-0219
17 *tcoates@msdlegal.com*

18 JOSEPH M. LYON (*pro hac vice* forthcoming)
19 **THE LYON FIRM, LLC**
20 2754 Erie Avenue
21 Cincinnati, OH 45208
22 Phone: (513) 381-2333
23 Fax: (513) 721-1178
24 *jlyon@thelyonfirm.com*

25 *Attorneys for Plaintiffs and the Proposed Class*

26 **UNITED STATES DISTRICT COURT**
27 **NORTHERN DISTRICT OF CALIFORNIA**

28 EVANGELIA REMOUNDOS, JOHN
BIEGGER, and ANNE BIEGGER, on behalf
of themselves and on behalf of all others
similarly situated,

Plaintiffs,

v.

LENDUS, LLC,

Defendant.

Case No.: 4:22-cv-00749

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Evangelia Remoundos, John Biegger, and Anne Biegger (“Plaintiffs”) bring this
Class Action Complaint against LendUS, LLC (“Defendant” or “LendUS”), in their individual

1 capacity and on behalf of all others similarly situated, and allege, upon personal knowledge as to
2 their own actions and their counsels’ investigations, and upon information and belief as to all other
3 matters, as follows:

4 **INTRODUCTION**

5 1. Defendant is a mortgage company based in Alamo, California.¹ It is the surviving
6 product of a merger between two mortgage companies.²

7 2. Plaintiffs bring this class action against Defendant for its failure to properly secure
8 and safeguard Personally Identifiable Information provided by its clients or mortgage brokers,
9 including, without limitation, first and last names, mailing addresses, dates of birth, Social Security
10 numbers, and tax information (“PII”).

11 3. On December 21, 2021, Defendant identified “unauthorized access” to LendUS
12 email accounts connected to its servers.³ It later learned that “an unauthorized person accessed
13 certain accounts at various times between February 2, 2021 and March 22, 2021,” and that PII
14 from its network may have been compromised (the “Data Breach”).⁴

15 4. Defendant failed to use reasonable industry standard security measures, which
16 would have prevented this type of attack from being successful. Defendant’s failure to use such
17 measures is particularly egregious given the amount of highly sensitive PII that it maintains and
18 the prevalence of data security incidents in the finance and banking industries.

19 5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and
20 Class Members, Defendant assumed legal and equitable duties to those individuals to protect and
21 safeguard that information from unauthorized access and intrusion.

22 6. Hackers can access and then offer for sale this unencrypted, unredacted PII to
23 criminals. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Plaintiffs
24 and Class Members now face a present and continuing lifetime risk of identity theft, which is

25 ¹ <https://www.lend.us/> (last visited Feb. 2, 2022).

26 ² *Id.*

27 ³ <https://apps.web.maine.gov/online/aeviewer/ME/40/3a0c4c95-a995-4ffb-88b4-57e8cc0ff702.shtml> (last
visited Feb. 2, 2022).

28 ⁴ *Id.*

1 heightened here by the loss of Social Security numbers.

2 7. Plaintiffs bring this action on behalf of all persons whose PII was compromised as
3 a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members;
4 (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices;
5 and (iii) effectively secure its network containing protected PII using reasonable and effective
6 security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to
7 negligence and violates federal and state statutes.

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

17 9. Defendant disregarded the rights of Plaintiffs and Class Members by recklessly or
18 negligently failing to implement and maintain adequate and reasonable measures to ensure that the
19 PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an
20 unauthorized disclosure of data, and failing to follow applicable, required, and appropriate
21 protocols, policies, and procedures regarding the encryption of data, even for internal use. As a
22 result, the PII of Plaintiffs and Class Members was compromised through disclosure to a known
23 criminal organization. Plaintiffs and Class Members have a continuing interest in ensuring that
24 their information is and remains safe, and they should be entitled to injunctive and other equitable
25 relief.

1 **PARTIES**

2 ***Plaintiff Evangelia Remoundos***

3 10. Plaintiff Evangelia Remoundos is, and at all times relevant has been, a resident and
4 citizen of San Francisco, California. Plaintiff received a “Notice of Data Breach” letter dated
5 January 19, 2022, on or about that date. The letter notified her that on December 21, 2021, LendUS
6 determined that in the compromised email accounts, information such as her full name and Social
7 Security Number had been accessed. The letter further advised that she should “remain vigilant by
8 reviewing” financial accounts and credit reports for signs of fraud.

9 11. Upon information and belief, Defendant continues to maintain Plaintiff
10 Remoundos’ PII.

11 ***Plaintiff John Biegger***

12 12. Plaintiff John Biegger was at all times relevant a resident and citizen of
13 Jacksonville, Florida. Plaintiff Biegger received a “Notice of Data Breach” letter dated January
14 19, 2022, on or about that date. The letter notified him that on December 21, 2021, LendUS
15 determined that in the compromised email accounts, information such as his full name, financial
16 account number, and payment card number had been accessed. The letter further advised that he
17 should “remain vigilant by reviewing” financial accounts and credit reports for signs of fraud.

18 13. Upon information and belief, Defendant continues to maintain Plaintiff Biegger’s
19 PII.

20 ***Plaintiff Anne Biegger***

21 14. Plaintiff Anne Biegger was at all times relevant a resident and citizen of
22 Jacksonville, Florida. Plaintiff Biegger received a “Notice of Data Breach” letter dated January
23 19, 2022, on or about that date. The letter notified her that on December 21, 2021, LendUS
24 determined that in the compromised email accounts, information such as her full name, financial
25 account number, and payment card number had been accessed. The letter further advised that she
26 should “remain vigilant by reviewing” financial accounts and credit reports for signs of fraud.

27 15. Upon information and belief, Defendant continues to maintain Plaintiff Biegger’s
28

1 PII.

2 ***Defendant LendUS, LLC***

3 16. Defendant LendUS, LLC is a California State registered mortgage company with
4 its principal office located at 3240 Stone Valley Road West, Alamo California 94507.

5 17. Upon information and belief, LendUS is an LLC created as a combination of RPM
6 Mortgage and American Eagle Mortgage.⁵ All of Plaintiffs' claims stated herein are asserted
7 against Defendant and any of its owners, predecessors, partners, successors, subsidiaries, agents
8 and/or assigns.

9 **JURISDICTION AND VENUE**

10 18. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.
11 § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or
12 value of \$5,000,000, exclusive of interest and costs, there are more than 100 members in the
13 proposed class, and at least one member of the class is a citizen of a state different from Defendant,
14 including Plaintiffs Mr. and Mrs. Biegger, who are residents of Florida.

15 19. This Court has personal jurisdiction over Defendant because Defendant has its
16 principal place of business within this District.

17 20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial
18 part of the events or omissions giving rise to these claims occurred in, were directed to, and/or
19 emanated from this District. Defendant resides within this judicial district and a substantial part of
20 the events giving rise to the claims alleged herein occurred within this judicial district.

21 **FACTUAL ALLEGATIONS**

22 ***Background***

23 21. Defendant provides various mortgage and loan services to individuals in several
24 states across the country, including its home state of California. It offers an app and various
25 educational tools to help assist first time homebuyers, or buyers proceeding without the assistance
26

27 _____
28 ⁵ <https://www.lend.us/> (last visited Feb. 2, 2022).

1 of a financial advisor, as well as various financing or refinancing services for experienced
2 homebuyers.

3 22. Plaintiffs and Class Members, however, were not direct customers of Defendant.

4 23. Plaintiffs and Class Members and/or Plaintiffs’ and Class Members’ agents or
5 employers relied on the sophistication of Defendant to keep their PII confidential and securely
6 maintained, to use this information for business purposes only, and to make only authorized
7 disclosures of this information. Plaintiffs and Class Members demand security to safeguard their
8 PII.

9 24. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs
10 and Class Members from involuntary disclosure to third parties.

11 ***The Data Breach***

12 25. On December 21, 2021, Defendant identified “unauthorized access to some
13 LendUS employee email accounts.”⁶ According to Defendant, it then “took immediate steps to
14 secure the email accounts and began an investigation.”⁷ However, it has not stated when the
15 unusual activity first occurred.

16 26. The unauthorized access to Defendant’s email accounts occurred between February
17 2, 2021 and March 22, 2021 – at least nine months before LendUS even discovered that the
18 unauthorized access occurred.⁸

19 27. Despite a protracted investigation into the Data Breach, assisted by the services of
20 an unnamed cybersecurity firm, Defendant was unable to determine what emails, attachments, or
21 other data might have been downloaded by the unauthorized assailant.

22 28. Defendant failed to use reasonable industry standard security measures, which
23 would have prevented this type of attack. Defendant’s failure to use such measures is particularly
24

25 ⁶ <https://www.jdsupra.com/legalnews/data-breach-alert-lendus-llc-3790258/#:~:text=If%20you%20receive%20a%20data,retained%20your%20sensitive%20personal%20in>
26 formation. (Last visited Feb. 2, 2022).

27 ⁷ *Id.*

28 ⁸ *Id.*

1 egregious given the amount of highly sensitive PII that it maintains and the prevalence of data
2 security incidents in the finance and banking industries.

3 29. In notice letters subsequently sent to victims of the Data Breach, Defendant
4 acknowledged its duty to safeguard the PII in its possession: “The privacy and security of
5 information entrusted to us is of the utmost importance to LENDUS, and we take this incident very
6 seriously.... Please know that the security of your information is of paramount importance to us,
7 and we deeply regret any worry or inconvenience this incident may have caused.”⁹

8 30. The notice letters sent to victims of the Data Breach also acknowledged that its
9 previous cybersecurity policies and procedures were lacking and need improvement: “[W]e are
10 working to review our existing policies and procedures, including our information security plan,
11 to evaluate additional measures and safeguards to protect against this type of incident in the
12 future.”¹⁰

13 31. The notice letters to victims of the Data Breach did not provide the details of the
14 Data Breach, the vulnerabilities exploited, or the remedial measures undertaken to ensure such a
15 breach does not occur again.

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

20 33. Defendant did not use reasonable security procedures and practices appropriate to
21 the nature of the sensitive information it was maintaining for Plaintiffs and Class Members,
22 causing the exposure of PII for many customers and/or its customers’ employees, such as
23 encrypting the information or deleting it when it is no longer needed. ¹¹

24 _____
25 ⁹

26 https://oag.ca.gov/system/files/001%20LendUS%20CA%20Adult%20CA%20CM%201%20YR_AF443_v02.pdf (last visited Feb. 2, 2022).

27 ¹⁰ *Id.*

28 ¹¹ It is clear that the information exposed in the Data Breach was unencrypted: California law requires companies to notify California residents “whose **unencrypted** personal information was, or is reasonably

1 34. As explained by the Federal Bureau of Investigation, “[p]revention is the most
2 effective defense against ransomware and it is critical to take precautions for protection.”¹²

3 35. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could
4 and should have implemented, as recommended by the United States Government, the following
5 measures:

- 6 • Implement an awareness and training program. Because end users are targets,
7 employees and individuals should be aware of the threat of ransomware and
8 how it is delivered.
- 9 • Enable strong spam filters to prevent phishing emails from reaching the end
10 users and authenticate inbound email using technologies like Sender Policy
11 Framework (SPF), Domain Message Authentication Reporting and
12 Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent
13 email spoofing.
- 14 • Scan all incoming and outgoing emails to detect threats and filter executable
15 files from reaching end users.
- 16 • Configure firewalls to block access to known malicious IP addresses.
- 17 • Patch operating systems, software, and firmware on devices. Consider using a
18 centralized patch management system.
- 19 • Set anti-virus and anti-malware programs to conduct regular scans
20 automatically.
- 21 • Manage the use of privileged accounts based on the principle of least privilege:
22 no users should be assigned administrative access unless absolutely needed;
23 and those with a need for administrator accounts should only use them when
24 necessary.

25 _____
26 believed to have been, acquired by an unauthorized person” due to a “breach of the security of the system[.]”
27 Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of
28 the Data Breach on Jan. 19, 2022, evidencing that the exposed data was unencrypted.

¹² How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Feb. 2, 2022).

- 1 • Configure access controls—including file, directory, and network share
2 permissions—with least privilege in mind. If a user only needs to read specific
3 files, the user should not have written access to those files, directories, or
4 shares.
- 5 • Disable macro scripts from office files transmitted via email. Consider using
6 Office Viewer software to open Microsoft Office files transmitted via email
7 instead of full office suite applications.
- 8 • Implement Software Restriction Policies (SRP) or other controls to prevent
9 programs from executing from common ransomware locations, such as
10 temporary folders supporting popular Internet browsers or
11 compression/decompression programs, including the AppData/LocalAppData
12 folder.
- 13 • Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- 14 • Use application whitelisting, which only allows systems to execute programs
15 known and permitted by security policy.
- 16 • Execute operating system environments or specific programs in a virtualized
17 environment.
- 18 • Categorize data based on organizational value and implement physical and
19 logical separation of networks and data for different organizational units.¹³

20 36. To prevent and detect cyber-attacks Defendant could and should have
21 implemented, as recommended by the United States Cybersecurity & Infrastructure Security
22 Agency, the following measures:

- 23 • **Update and patch your computer.** Ensure your applications and operating systems
24 (OSs) have been updated with the latest patches. Vulnerable applications and OSs are
25 the target of most ransomware attacks....
- 26 • **Use caution with links and when entering website addresses.** Be careful when
27 clicking directly on links in emails, even if the sender appears to be someone you
28 know. Attempt to independently verify website addresses (e.g., contact your

¹³ *Id.* at 3-4.

1 organization's helpdesk, search the internet for the sender organization's website or
2 the topic mentioned in the email). Pay attention to the website addresses you click on,
3 as well as those you enter yourself. Malicious website addresses often appear almost
4 identical to legitimate sites, often using a slight variation in spelling or a different
5 domain (e.g., .com instead of .net)....

- 6 • **Open email attachments with caution.** Be wary of opening email attachments, even
7 from senders you think you know, particularly when attachments are compressed files
8 or ZIP files.
- 9 • **Keep your personal information safe.** Check a website's security to ensure the
10 information you submit is encrypted before you provide it....
- 11 • **Verify email senders.** If you are unsure whether or not an email is legitimate, try to
12 verify the email's legitimacy by contacting the sender directly. Do not click on any
13 links in the email. If possible, use a previous (legitimate) email to ensure the contact
14 information you have for the sender is authentic before you contact them.
- 15 • **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to
16 date on ransomware techniques. You can find information about known phishing
17 attacks on the Anti-Phishing Working Group website. You may also want to sign up
18 for CISA product notifications, which will alert you when a new Alert, Analysis
19 Report, Bulletin, Current Activity, or Tip has been published.
- 20 • **Use and maintain preventative software programs.** Install antivirus software,
21 firewalls, and email filters—and keep them updated—to reduce malicious network
22 traffic....¹⁴

23 37. To prevent and detect cyber-attacks or ransomware attacks Defendant could and
24 should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team,
25 the following measures:

26 **Secure internet-facing assets**

- 27 -Apply latest security updates
- 28 -Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full
compromise;

¹⁴ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019),
available at: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Feb. 2, 2022).

1 **Include IT Pros in security discussions**

- 2 - Ensure collaboration among [security operations], [security admins], and
3 [information technology] admins to configure servers and other endpoints
4 securely;

5 **Build credential hygiene**

- 6 - Use [multifactor authentication] or [network level authentication] and use
7 strong, randomized, just-in-time local admin passwords;

8 **Apply principle of least-privilege**

- 9 - Monitor for adversarial activities
10 - Hunt for brute force attempts
11 - Monitor for cleanup of Event Logs
12 - Analyze logon events;

13 **Harden infrastructure**

- 14 - Use Windows Defender Firewall
15 - Enable tamper protection
16 - Enable cloud-delivered protection
17 - Turn on attack surface reduction rules and [Antimalware Scan Interface] for
18 Office [Visual Basic for Applications].¹⁵

19 38. The occurrence of the Data Breach indicates that Defendant failed to adequately
20 implement one or more of the above measures to prevent ransomware attacks, resulting in the Data
21 Breach and the exposure of the PII of at least 12,000 individuals, including Plaintiffs and Class
22 Members.

23 ***Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members***

24 39. Defendant has historically acquired, collected, and stored the PII of Plaintiffs and
25 Class Members.

26 40. As part of receiving services from Defendant, Plaintiffs and Class Members and/or
27 Plaintiffs' and Class Members' agents or employers, as customers of Defendant, are required to
28 give their sensitive and confidential PII to Defendant. Defendant retains this information.

 41. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members,

¹⁵ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Feb. 2, 2022).

1 Defendant assumed legal and equitable duties and knew or should have known that it was
2 responsible for protecting the PII from disclosure.

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

7 43. Defendant could have prevented this Data Breach by properly and adequately
8 securing and encrypting the files and file servers containing the PII of Plaintiffs and Class
9 Members.

10 44. Defendant's policies on its website include promises and legal obligations to
11 maintain and protect PII, demonstrating an understanding of the importance of securing PII.
12 Indeed, Defendant has an entire page of its website dedicated to cybersecurity awareness.¹⁶

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

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

18 ***Defendant Knew or Should Have Known of the Risk Because the Financial Industry is***
19 ***Particularly Susceptible to Cyber Attacks***

20 47. Defendant knew and understood unprotected or exposed PII in the custody of
21 banks, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to
22 illegally monetize that PII through unauthorized access.

23 48. Defendant had obligations created by contract, industry standards, common law,
24 and representations made to Plaintiffs and Class Members and/or to Plaintiffs' and Class
25 Members' agents or employers, and the general public, to keep their PII confidential and to
26

27 ¹⁶ See <https://www.lend.us/PDFs/lendus-privacy.pdf>; <https://www.lend.us/ccpa/> (last visited Feb. 2,
28 2022).

1 protect it from unauthorized access and disclosure.

2 49. Plaintiffs and Class Members and/or Plaintiffs' and Class Members' agents or
3 employers, provided their PII to Defendant with the reasonable expectation and mutual
4 understanding that Defendant would comply with their obligations to keep such information
5 confidential and secure from unauthorized access.

6 50. Defendant's data security obligations were particularly important given the
7 substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

8 51. Indeed, data breaches, such as the one experienced by Defendant, have become
9 so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued
10 a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore,
11 the increase in such attacks, and attendant risk of future attacks, was widely known and
12 completely foreseeable to the public, including Defendant.

13 52. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc
14 on consumers' finances, credit history, and reputation and can take time, money, and patience to
15 resolve.¹⁷ Identity thieves use stolen personal information for a variety of crimes, including
16 credit card fraud, phone or utilities fraud, and bank and finance fraud.¹⁸

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

20 54. Defendant knew, or reasonably should have known, of the importance of
21

22 ¹⁷ See *Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013),
23 <https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf> (last visited Feb. 2, 2022).

24 ¹⁸ *Id.* The FTC defines identity theft as "a fraud committed or attempted using the
25 identifying information of another person without authority." 16 CFR § 603.2. The FTC
26 describes "identifying information" as "any name or number that may be used, alone or in
27 conjunction with any other information, to identify a specific person," including, among other
28 things, "[n]ame, social security number, date of birth, official State or government issued driver's
license or identification number, alien registration number, government passport number,
employer or taxpayer identification number." *Id.*

1 safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that
2 would occur if Defendant's data security systems were breached, including, specifically, the
3 significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

8 56. The injuries to Plaintiffs and Class Members were directly and proximately caused
9 by Defendant's failure to implement or maintain adequate data security measures for the PII of
10 Plaintiffs and Class Members, such as encrypting the data so unauthorized third parties could not
11 see the PII.

12 ***Defendant Failed to Comply with Industry Standards***

13 57. A number of industry and national best practices have been published and should
14 have been used as a go-to resource and authoritative guide when developing Defendant's
15 cybersecurity practices.

16 58. Best cybersecurity practices that are standard include installing appropriate
17 malware detection software; monitoring and limiting the network ports; protecting web browsers
18 and email management systems; setting up network systems such as firewalls, switches and
19 routers; monitoring and protection of physical security systems; protection against any possible
20 communication system; and training staff regarding critical points.

21 59. Upon information and belief, Defendant failed to meet the minimum standards of
22 the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1
23 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,
24 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8,
25 and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC),
26 which are established standards in reasonable cybersecurity readiness.

27 60. These foregoing frameworks are existing and applicable industry standards in
28

1 Defendant’s industry, and Defendant failed to comply with these accepted standards, thereby
2 opening the door to a cyber-attack and causing the Data Breach.

3 ***Value of Personally Identifiable Information***

4 61. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud
5 committed or attempted using the identifying information of another person without authority.”¹⁹
6 The FTC describes “identifying information” as “any name or number that may be used, alone or
7 in conjunction with any other information, to identify a specific person,” including, among other
8 things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s
9 license or identification number, alien registration number, government passport number,
10 employer or taxpayer identification number.”²⁰

11 62. The PII of individuals remains of high value to criminals, as evidenced by the prices
12 they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity
13 credentials. For example, Personal Information can be sold at a price ranging from \$40 to \$200,
14 and bank details have a price range of \$50 to \$200.²¹ Experian reports that a stolen credit or debit
15 card number can sell for \$5 to \$110 on the dark web.²² Criminals can also purchase access to entire
16 company data breaches from \$900 to \$4,500.²³

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

21 A dishonest person who has your Social Security number can use it to get other
22

23 ¹⁹ 17 C.F.R. § 248.201 (2013).

24 ²⁰ *Id.*

25 ²¹ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019,
26 available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Feb. 2, 2022).

27 ²² *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017,
28 available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 2, 2022).

²³ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Feb. 2, 2022).

1 personal information about you. Identity thieves can use your number and your
2 good credit to apply for more credit in your name. Then, they use the credit cards
3 and don't pay the bills, it damages your credit. You may not find out that someone
4 is using your number until you're turned down for credit, or you begin to get calls
5 from unknown creditors demanding payment for items you never bought. Someone
6 illegally using your Social Security number and assuming your identity can cause
7 a lot of problems.²⁴

8 64. It is no easy task to change or cancel a stolen Social Security number. An individual
9 cannot obtain a new Social Security number without significant paperwork and evidence of actual
10 misuse. In other words, preventive action to defend against the possibility of misuse of a Social
11 Security number is not permitted; an individual must show evidence of actual, ongoing fraud
12 activity to obtain a new number.

13 65. Even then, a new Social Security number may not be effective. According to Julie
14 Ferguson of the Identity Theft Resource Center, “[t]he credit bureaus and banks are able to link
15 the new number very quickly to the old number, so all of that old bad information is quickly
16 inherited into the new Social Security number.”²⁵

17 66. Based on the foregoing, the information compromised in the Data Breach is
18 significantly more valuable than the loss of, for example, credit card information in a retailer data
19 breach because, there, victims can cancel or close credit and debit card accounts. The information
20 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
21 change—Social Security number, driver’s license number, name, and date of birth.

22 67. This data demands a much higher price on the black market. Martin Walter, senior
23 director at cybersecurity firm RedSeal, explained, “Compared to credit card information,
24 personally identifiable information and Social Security numbers are worth more than 10x on the
25 black market.”²⁶

26 ²⁴ Social Security Administration, *Identity Theft and Your Social Security Number*, available at:
27 <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Feb. 2, 2022).

28 ²⁵ 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 visited Feb. 2, 2022).

²⁶ 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 visited Feb. 2, 2022).

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

3 69. The fraudulent activity resulting from the Data Breach may not come to light for
4 years.

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

8 [L]aw enforcement officials told us that in some cases, stolen data may be held for
9 up to a year or more before being used to commit identity theft. Further, once stolen
10 data have been sold or posted on the Web, fraudulent use of that information may
11 continue for years. As a result, studies that attempt to measure the harm resulting
12 from data breaches cannot necessarily rule out all future harm.²⁷

13 71. At all relevant times, Defendant knew, or reasonably should have known, of the
14 importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security
15 numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant’s
16 data security system was breached, including, specifically, the significant costs that would be
17 imposed on Plaintiffs and Class Members as a result of a breach.

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

21 73. Defendant was, or should have been, fully aware of the unique type and the
22 significant volume of data on Defendant’s server(s), amounting to potentially thousands of
23 individuals’ detailed, PII, and, thus, the significant number of individuals who would be harmed
24 by the exposure of the unencrypted data.

25 74. In the breach notification letter, Defendant made an offer of 12 months of credit
26 monitoring and identity theft services. This is wholly inadequate to compensate Plaintiffs and

27 ²⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
28 <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Feb. 2, 2022).

1 Class Members as it fails to provide for the fact that victims of data breaches and other
2 unauthorized disclosures commonly face multiple years of ongoing identity theft, and medical and
3 financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release
4 and disclosure of Plaintiffs' and Class Members' PII.

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

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

11 ***Defendant Violated the FTC Act***

12 77. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or
13 affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice
14 by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC
15 publications and orders described above also form part of the basis of Defendant's duty in this
16 regard.

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

22 ***Plaintiff Evangelia Remoundos' Experience***

23 79. Plaintiff Remoundos' PII was acquired by Defendant. The PII included her name,
24 Social Security number, tax returns, IRS Form W-2, payroll records, and other tax information and
25 her dependents' PII.
26
27
28

1 80. To date, LendUS has done next to nothing to adequately protect Plaintiff
2 Remoundos and Class Members, or to compensate them for their injuries sustained in this Data
3 Breach.

4 81. Defendant’s data breach notice letter downplays the theft of Plaintiff Remoundos’
5 and Class Members’ PII, when the facts demonstrate that the PII was targeted, accessed, and
6 exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by
7 Defendant are only for one year, and it places the burden squarely on Plaintiffs and Class Members
8 by requiring them to expend time signing up for the service and addressing timely issues when the
9 service number for enrollment does not work properly.

10 82. Plaintiff Remoundos and Class Members have been further damaged by the
11 compromise of their PII.

12 83. Plaintiff Remoundos’ PII was compromised in the Data Breach and was likely
13 stolen and in the hands of cybercriminals who illegally accessed LendUS’s network for the specific
14 purpose of targeting the PII.

15 84. Plaintiff Remoundos typically takes measures to protect her PII and is very careful
16 about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or
17 other unsecured source.

18 85. Plaintiff Remoundos stores any documents containing her PII in a safe and secure
19 location. And she diligently chooses unique usernames and passwords for her online accounts.

20 86. As a result of the Data Breach, Plaintiff Remoundos has suffered a loss of time and
21 has spent and continues to spend a considerable amount of time on issues related to this Data
22 Breach. She monitors her accounts and credit scores and has sustained emotional distress.
23 Furthermore, as the head of the household she has spent time assisting her dependents to
24 understand the Data Breach and has assisted them in applying for credit monitoring services. This
25 is time that was lost and unproductive and took away from other activities and work duties.

26 87. Plaintiff Remoundos also suffered actual injury in the form of damages to and
27 diminution in the value of her PII—a form of intangible property that she entrusted to Defendant
28

1 for the purpose of obtaining services from Defendant, which was compromised in and as a result
2 of the Data Breach.

3 88. Plaintiff Remoundos suffered lost time, annoyance, interference, and
4 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
5 of her privacy.

6 89. Plaintiff Remoundos has suffered continuing and certainly imminent and
7 impending injury arising from the substantially increased risk of fraud, identity theft, and misuse
8 resulting from her PII, especially her Social Security Number, being placed in the hands of
9 criminals.

10 90. Defendant obtained and continues to maintain Plaintiff Remoundos' PII and has a
11 continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.
12 She would have retrieved her and her dependents' PII from Defendant had she known that it would
13 fail to maintain adequate data security. Her PII was compromised and disclosed as a result of the
14 Data Breach.

15 91. As a result of the Data Breach, Plaintiff Remoundos anticipates spending
16 considerable time and money on an ongoing basis to try to mitigate and address harms caused by
17 the Data Breach. As a result of the Data Breach, she is at a present risk and will continue to be at
18 increased risk of identity theft and fraud for years to come.

19 ***Plaintiff John Biegger Experience***

20 92. Plaintiff Biegger was required to provide his PII to his mortgage company, RPM
21 Mortgage as part of a mortgage application.²⁸ The PII included his full name, address, Social
22 Security number, tax returns, IRS Form W-2, payroll records, and other tax information.

23 93. Plaintiff Biegger's PII was compromised in the Data Breach and was likely stolen
24 and in the hands of cybercriminals who illegally accessed LendUS's network for the specific
25 purpose of targeting the PII.

26
27
28 ²⁸ RPM Mortgage is a division of LendUS. <https://www.rpm-mtg.com/#about> (last visited Feb. 2, 2022).

1 94. Plaintiff Biegger typically takes measures to protect his PII and is very careful about
2 sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or other
3 unsecured source.

4 95. Plaintiff Biegger stores any documents containing his PII in a safe and secure
5 location and he diligently chooses unique usernames and passwords for online accounts.

6 96. As a result of the Data Breach, Plaintiff Biegger has suffered a loss of time and has
7 spent and continues to spend a considerable amount of time on issues related to this Data Breach.
8 He monitors accounts and credit scores and has sustained emotional distress.

9 97. Plaintiff Biegger also suffered actual injury in the form of damages to and
10 diminution in the value of his PII—a form of intangible property that he entrusted to Defendant
11 for the purpose of obtaining services from Defendant, which was compromised in and as a result
12 of the Data Breach.

13 98. Plaintiff Biegger suffered lost time, annoyance, interference, and inconvenience as
14 a result of the Data Breach and has anxiety and increased concerns for the loss of privacy.

15 99. Plaintiff Biegger has suffered continuing and certainly imminent and impending
16 injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting
17 from his PII, especially his Social Security Number, being placed in the hands of criminals.

18 100. Defendant obtained and continues to maintain Plaintiff Biegger's PII and has a
19 continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.
20 Defendant required the PII from him when he received services from Defendant. However, he
21 would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate
22 data security. His PII was compromised and disclosed as a result of the Data Breach.

23 101. As a result of the Data Breach, Plaintiff Biegger anticipates spending considerable
24 time and money on an ongoing basis to try to mitigate and address harms caused by the Data
25 Breach. As a result of the Data Breach, he is at a present risk and will continue to be at increased
26 risk of identity theft and fraud for years to come.

1 ***Plaintiff Anne Biegger Experience***

2 102. Plaintiff Anne Biegger was required to provide her PII to RPM Mortgage as part of
3 a mortgage application. The PII included her full name, address, Social Security number, tax
4 returns, IRS Form W-2, payroll records, and other tax information.

5 103. Plaintiff Anne Biegger’s PII was compromised in the Data Breach and was likely
6 stolen and in the hands of cybercriminals who illegally accessed LendUS’s network for the specific
7 purpose of targeting the PII.

8 104. Plaintiff Anne Biegger typically takes measures to protect her PII and is very
9 careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the
10 internet or other unsecured source.

11 105. Plaintiff Anne Biegger stores any documents containing her PII in a safe and secure
12 location and he diligently chooses unique usernames and passwords for online accounts.

13 106. As a result of the Data Breach, Plaintiff Anne Biegger has suffered a loss of time
14 and has spent and continues to spend a considerable amount of time on issues related to this Data
15 Breach. She monitors accounts and credit scores and has sustained emotional distress.

16 107. Plaintiff Anne Biegger also suffered actual injury in the form of damages to and
17 diminution in the value of her PII—a form of intangible property that she entrusted to Defendant
18 for the purpose of obtaining services from Defendant, which was compromised in and as a result
19 of the Data Breach.

20 108. Plaintiff Anne Biegger suffered lost time, annoyance, interference, and
21 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
22 of privacy.

23 109. Plaintiff Anne Biegger has suffered continuing and certainly imminent and
24 impending injury arising from the substantially increased risk of fraud, identity theft, and misuse
25 resulting from her PII, especially his Social Security number, being placed in the hands of
26 criminals.

1 Classes before the Court determines whether certification is appropriate.

2 117. Numerosity: The members of the Classes are so numerous that joinder of all
3 members is impracticable, if not completely impossible. The Classes are apparently identifiable
4 within Defendant's records.

5 118. Commonality: Common questions of law and fact exist as to all members of the
6 Classes and predominate over any questions affecting solely individual members of the Classes.
7 Among the questions of law and fact common to the Classes that predominate over questions
8 which may affect individual Class Members, including the following:

- 9 a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and
10 Class Members;
- 11 b. Whether Defendant had a duty not to disclose the PII of Plaintiffs and Class Members
12 to unauthorized third parties;
- 13 c. Whether Defendant had a duty not to use the PII of Plaintiffs and Class Members for
14 non-business purposes;
- 15 d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class
16 Members;
- 17 e. Whether and when Defendant actually learned of the Data Breach;
- 18 f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and
19 Class Members that their PII had been compromised;
- 20 g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class
21 Members that their PII had been compromised;
- 22 h. Whether Defendant failed to implement and maintain reasonable security procedures
23 and practices appropriate to the nature and scope of the information compromised in
24 the Data Breach;
- 25 i. Whether Defendant adequately addressed and fixed the vulnerabilities which
26 permitted the Data Breach to occur;
- 27 j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to
28

1 safeguard the PII of Plaintiffs and Class Members;

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

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

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

8 119. Typicality: Plaintiffs’ claims are typical of those of the other members of the
9 Classes because Plaintiffs, like every other member, were exposed to virtually identical conduct
10 and now suffers from the same violations of the law as other members of the Classes.

11 120. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests
12 of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to
13 those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the
14 Class Members and the infringement of the rights and the damages they have suffered are typical
15 of other Class Members. Plaintiffs have retained counsel experienced in complex class action
16 litigation, and Plaintiffs intend to prosecute this action vigorously.

17 121. Superiority and Manageability: Under Rule 23(b)(3), a class action is superior to
18 other available methods for the fair and efficient adjudication of this controversy since joinder of
19 all the members of the Classes is impracticable. Individual damages for any individual Class
20 Member are likely to be insufficient to justify the cost of individual litigation, so that in the absence
21 of class treatment, Defendant’s misconduct would go unpunished. Furthermore, the adjudication
22 of this controversy through a class action will avoid the possibility of inconsistent and potentially
23 conflicting adjudication of the asserted claims. There will be no difficulty in the management of
24 this action as a class action.

25 122. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because
26 Defendant has acted or refused to act on grounds generally applicable to the Classes, so that final
27 injunctive relief or corresponding declaratory relief is appropriate as to the Classes as a whole.
28

1 that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

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

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

11 130. Defendant also had a duty to exercise appropriate clearinghouse practices to remove
12 former customers' PII that Defendant was no longer required to retain pursuant to regulations or
13 legitimate business purposes.

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

16 132. Defendant's duty to use reasonable security measures arose as a result of the special
17 relationship that existed between Defendant on the one hand and Plaintiffs and the Class on the
18 other. That special relationship arose because Plaintiffs and the Class entrusted Defendant with
19 their confidential PII, a necessary part receiving services from Defendant.

20 133. Defendant was subject to an "independent duty," untethered to any contract
21 between Defendant and Plaintiffs or the Class.

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

25 135. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate
26 security practices and procedures. Defendant knew or should have known of the inherent risks in
27 collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing
28

1 adequate security of that information, and the necessity for encrypting or redacting PII stored on
2 Defendant's systems.

3 136. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the
4 Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and
5 opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included
6 its decisions to not comply with industry standards for the safekeeping of the PII of Plaintiffs and
7 the Class, including basic encryption techniques freely available to Defendant.

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

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

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

17 140. Defendant had a duty to employ proper procedures to prevent the unauthorized
18 dissemination of the PII of Plaintiffs and the Class.

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

21 142. Defendant, through its actions and/or omissions, unlawfully breached its duties to
22 Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in
23 protecting and safeguarding the PII of Plaintiffs and the Class during the time the PII was within
24 Defendant's possession or control.

25 143. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the
26 Class in deviation of standard industry rules, regulations, and practices at the time of the Data
27 Breach.

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

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

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

9 147. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and
10 the Class, the PII of Plaintiffs and the Class would not have been compromised.

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

16 149. Defendant's violation of California and federal statutes also constitute negligence
17 *per se*. Specifically, as described herein, Defendant has violated California's data breach statute,
18 Cal. Civ. Code § 1798.81.5, which requires Defendant to undertake reasonable measures to
19 safeguard the PII of Plaintiffs and the Class, as well as the FTC Act.

20 150. As a direct and proximate result of Defendant's negligence and negligence *per se*,
21 Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual
22 identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise,
23 publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,
24 detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost
25 opportunity costs associated with effort expended and the loss of productivity addressing and
26 attempting to mitigate the actual present and future consequences of the Data Breach, including
27 but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax
28

1 fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the
2 continued risk to their PII, which remain in Defendant’s possession and is subject to further
3 unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate
4 measures to protect the PII of Plaintiffs and the Class; and (viii) costs in terms of time, effort, and
5 money that will be expended to prevent, detect, contest, and repair the impact of the PII
6 compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the
7 Class.

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

12 152. Additionally, as a direct and proximate result of Defendant’s negligence and
13 negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of
14 exposure of their PII, which remain in Defendant’s possession and is subject to further
15 unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures
16 to protect the PII in its continued possession.

17 153. Plaintiffs and Class Members are therefore entitled to damages, including
18 restitution and unjust enrichment, declaratory and injunctive relief, and attorneys’ fees, costs, and
19 expenses.

20 **COUNT II**
21 **CALIFORNIA CONSUMER PRIVACY ACT**
22 **(On Behalf of Plaintiff Remoundos and the California Subclass)**

23 154. Plaintiff Remoundos and the California Subclass re-allege and incorporate by
24 reference herein all of the allegations contained in paragraphs 1 through 153.

25 155. Defendant violated section 1798.150(a) of the California Consumer Privacy Act
26 (“CCPA”) by failing to prevent Plaintiff Remoundos’ and the California Subclass’ PII from
27 unauthorized access and exfiltration, theft, or disclosure as a result of Defendant’s violations of its
28

1 duty to implement and maintain reasonable security procedures and practices appropriate to the
2 nature of the information to protect the PII.

3 156. The PII of Plaintiff Remoundos and the California Subclass was subjected to
4 unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of
5 Defendant's violation of its duty under the CCPA.

6 157. Plaintiff Remoundos and the California Subclass lost money or property, including
7 but not limited to the loss of legally protected interest in the confidentiality and privacy of their
8 PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts
9 described above.

10 158. Defendant knew, or should have known, that their network computer systems and
11 data security practices were inadequate to safeguard PII and that the risk of a data breach or theft
12 was highly likely. Defendant failed to implement and maintain reasonable security procedures and
13 practices appropriate to the nature of the information to protect PII, such as properly encrypting
14 the PII so in the event of a data breach the PII cannot be read by an unauthorized third party. As a
15 result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff
16 Remoundos and members of the California Subclass was exposed.

17 159. Defendant is organized for the profit or financial benefit of its owners and collects
18 PII as defined in Cal. Civ. Code section 1798.140.

19 160. Plaintiff Remoundos and the California Subclass seek injunctive or other equitable
20 relief to ensure that Defendant hereinafter adequately safeguard PII by implementing reasonable
21 security procedures and practices. This relief is important because Defendant still holds PII related
22 to Plaintiff Remoundos and the California Subclass. Plaintiff Remoundos and the California
23 Subclass have an interest in ensuring that their PII is reasonably protected.

24 161. On February 4, 2022, Plaintiffs' counsel mailed a CCPA notice letter to Defendant
25 via certified mail. If Defendant does not cure the effects of the Data Breach, which would require
26 retrieving the PII or securing the PII from continuing and future use, within 30 days of delivery of
27 the CCPA notice letter (which Plaintiff Remoundos believes any such cure is not possible under
28

1 these facts and circumstances), Plaintiff Remoundos intends to amend this complaint to seek actual
2 damages and statutory damages of no less than \$100 and up to \$750 per customer record subject
3 to the Data Breach on behalf of the California Subclass as authorized by the CCPA.

4 **COUNT III**
5 **VIOLATIONS OF CALIFORNIA’S UNFAIR COMPETITION LAW**
6 **Cal. Bus. & Prof. Code § 17200, *et seq.***
7 **(On Behalf of Plaintiff Remoundos and the California Subclass)**

8 162. Plaintiff Remoundos re-alleges and incorporates by reference herein all of the
9 allegations contained in paragraphs 1 through 161.

10 163. By reason of the conduct alleged herein, Defendant engaged in unlawful and unfair
11 business practices within the meaning of California’s Unfair Competition Law (“UCL”), Business
12 and Professions Code § 17200, *et seq.*

13 164. Defendant stored the PII of Plaintiff Remoundos and Subclass Members in its
14 computer systems.

15 165. Defendant knew or should have known it did not employ reasonable, industry
16 standard, and appropriate security measures that complied with federal regulations and that would
17 have kept Plaintiff Remoundos’ and Subclass Members’ PII secure and prevented the loss or
18 misuse of that PII.

19 166. Defendant did not disclose at any time that Plaintiff Remoundos’ and Subclass
20 Members’ PII was vulnerable to hackers because Defendant’s data security measures were
21 inadequate and outdated, and Defendant was the only one in possession of that material
22 information, which Defendant had a duty to disclose.

23 ***Unlawful Business Practices***

24 167. Defendant engaged in unlawful business acts and practices by failing to establish
25 adequate security practices and procedures as set forth above, by soliciting and gathering the PII
26 of Plaintiff Remoundos and the Subclass knowing that the information would not be adequately
27 protected, and by storing the PII of Plaintiff Remoundos and the Subclass in an unsecure electronic
28 network, all in violation of California’s data breach statute, Cal. Civ. Code § 1798.81.5, which

1 requires Defendant to undertake reasonable measures to safeguard the PII of Plaintiff Remoundos
2 and the Subclass, as well as the FTC Act.

3 168. Plaintiff Remoundos and Subclass Members suffered injury in fact and lost money
4 or property as the result of Defendant’s unlawful business practices. In addition, Plaintiff
5 Remoundos’ and Subclass Members’ PII was taken and is in the hands of those who will use it for
6 their own advantage, or is being sold for value, making it clear that the hacked information is of
7 tangible value. Plaintiff Remoundos and Subclass Members have also suffered consequential out
8 of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and
9 other expenses relating to identity theft losses or protective measures.

10 ***Unfair Business Practices***

11 169. Defendant engaged in unfair business practices under the “balancing test.” The
12 harm caused by Defendant’s actions and omissions, as described in detail above, greatly outweigh
13 any perceived utility. Indeed, Defendant’s failure to follow basic data security protocols and failure
14 to disclose inadequacies of Defendant’s data security cannot be said to have had any utility at all.
15 All of these actions and omissions were clearly injurious to Plaintiff Remoundos and Subclass
16 Members, directly causing the harms alleged below.

17 170. Defendant engaged in unfair business practices under the “tethering test.”
18 Defendant’s actions and omissions, as described in detail above, violated fundamental public
19 policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The
20 Legislature declares that . . . all individuals have a right of privacy in information pertaining to
21 them The increasing use of computers . . . has greatly magnified the potential risk to individual
22 privacy that can occur from the maintenance of personal information.”); Cal. Civ. Code
23 § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information about
24 California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the
25 Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide
26 concern.”). Defendant’s acts and omissions thus amount to a violation of the law.

- 1 iii. requiring Defendant to delete, destroy, and purge the personal identifying
2 information of Plaintiffs and Class Members unless Defendant can provide to
3 the Court reasonable justification for the retention and use of such information
4 when weighed against the privacy interests of Plaintiffs and Class Members;
5 iv. requiring Defendant to implement and maintain a comprehensive Information
6 Security Program designed to protect the confidentiality and integrity of the PII
7 of Plaintiffs and Class Members;
8 v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class
9 Members on a cloud-based database;
10 vi. requiring Defendant to engage independent third-party security
11 auditors/penetration testers as well as internal security personnel to conduct
12 testing, including simulated attacks, penetration tests, and audits on
13 Defendant's systems on a periodic basis, and ordering Defendant to promptly
14 correct any problems or issues detected by such third-party security auditors;
15 vii. requiring Defendant to engage independent third-party security auditors and
16 internal personnel to run automated security monitoring;
17 viii. requiring Defendant to audit, test, and train its security personnel regarding any
18 new or modified procedures;
19 ix. requiring Defendant to segment data by, among other things, creating firewalls
20 and access controls so that if one area of Defendant's network is compromised,
21 hackers cannot gain access to other portions of Defendant's systems;
22 x. requiring Defendant to conduct regular database scanning and securing checks;
23 xi. requiring Defendant to establish an information security training program that
24 includes at least annual information security training for all employees, with
25 additional training to be provided as appropriate based upon the employees'
26 respective responsibilities with handling personal identifying information, as
27 well as protecting the personal identifying information of Plaintiffs and Class
28

1 Members;

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

6 xiii. requiring Defendant to implement a system of tests to assess its employees'
7 knowledge of the education programs discussed in the preceding
8 subparagraphs, as well as randomly and periodically testing employees'
9 compliance with Defendant's policies, programs, and systems for protecting
10 personal identifying information;

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

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

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

26 D. For an award of damages, including actual, statutory, nominal, and consequential
27 damages, as allowed by law in an amount to be determined;
28

- 1 E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
2 F. For prejudgment interest on all amounts awarded; and,
3 G. Such other and further relief as this Court may deem just and proper.

4 **DEMAND FOR JURY TRIAL**

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

6 DATED: February 4, 2022

Respectfully Submitted,

7
8 By: /s/ M. Anderson Berry
9 M. ANDERSON BERRY (262879)
10 GREGORY HAROUTUNIAN (330263)
11 **CLAYEO C. ARNOLD,**
12 **A PROFESSIONAL LAW CORP.**
13 865 Howe Avenue
14 Sacramento, CA 95825
15 Telephone: (916) 239-4778
16 Facsimile: (916) 924-1829
17 *aberry@justice4you.com*
18 *gharoutunian@justice4you.com*

14 TERENCE R. COATES (*pro hac vice* forthcoming)
15 **MARKOVITS, STOCK & DEMARCO, LLC**
16 3825 Edwards Road, Suite 650
17 Cincinnati, OH 45209
18 Phone: (513) 665-0204
19 Fax: (513) 665-0219
20 *tcoates@msdlegal.com*

18 JOSEPH M. LYON (*pro hac vice* forthcoming)
19 **THE LYON FIRM, LLC**
20 2754 Erie Avenue
21 Cincinnati, OH 45208
22 Phone: (513) 381-2333
23 Fax: (513) 721-1178
24 *jlyon@thelyonfirm.com*

23 *Attorneys for Plaintiffs and the Proposed Class*

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

EVANGELIA REMOUNDOS, JOHN BIEGGER, and ANNE BIEGGER

(b) County of Residence of First Listed Plaintiff **San Francisco**
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)

M. Anderson Berry, Esq. (SBN 262879)
Clayeo C. Arnold, APLC dba Arnold Law Firm
865 Howe Avenue, Sacramento, CA 95825 Tel. (916) 239-4778; Fax (916) 924-1829
Email: aberry@justice4you.com

DEFENDANTS

LENDUS, LLC

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

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

- | | |
|--|--|
| <input type="checkbox"/> 1 U.S. Government Plaintiff | <input type="checkbox"/> 3 Federal Question
(U.S. Government Not a Party) |
| <input type="checkbox"/> 2 U.S. Government Defendant | <input checked="" type="checkbox"/> 4 Diversity
(Indicate Citizenship of Parties in Item III) |

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
<input type="checkbox"/> 110 Insurance	PERSONAL INJURY	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC § 881	<input type="checkbox"/> 422 Appeal 28 USC § 158	<input type="checkbox"/> 375 False Claims Act
<input type="checkbox"/> 120 Marine	<input type="checkbox"/> 310 Airplane	<input type="checkbox"/> 690 Other	<input type="checkbox"/> 423 Withdrawal 28 USC § 157	<input type="checkbox"/> 376 Qui Tam (31 USC § 3729(a))
<input type="checkbox"/> 130 Miller Act	<input type="checkbox"/> 315 Airplane Product Liability			<input type="checkbox"/> 400 State Reapportionment
<input type="checkbox"/> 140 Negotiable Instrument	<input type="checkbox"/> 320 Assault, Libel & Slander	LABOR	PROPERTY RIGHTS	<input type="checkbox"/> 410 Antitrust
<input type="checkbox"/> 150 Recovery of Overpayment of Veteran's Benefits	<input type="checkbox"/> 330 Federal Employers' Liability	<input type="checkbox"/> 710 Fair Labor Standards Act	<input type="checkbox"/> 820 Copyrights	<input type="checkbox"/> 430 Banks and Banking
<input type="checkbox"/> 151 Medicare Act	<input type="checkbox"/> 340 Marine	<input type="checkbox"/> 720 Labor/Management Relations	<input type="checkbox"/> 830 Patent	<input type="checkbox"/> 450 Commerce
<input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans)	<input type="checkbox"/> 345 Marine Product Liability	<input type="checkbox"/> 740 Railway Labor Act	<input type="checkbox"/> 835 Patent—Abbreviated New Drug Application	<input type="checkbox"/> 460 Deportation
<input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits	<input type="checkbox"/> 350 Motor Vehicle	<input type="checkbox"/> 751 Family and Medical Leave Act	<input type="checkbox"/> 840 Trademark	<input type="checkbox"/> 470 Racketeer Influenced & Corrupt Organizations
<input type="checkbox"/> 160 Stockholders' Suits	<input type="checkbox"/> 355 Motor Vehicle Product Liability	<input type="checkbox"/> 790 Other Labor Litigation	<input type="checkbox"/> 880 Defend Trade Secrets Act of 2016	<input type="checkbox"/> 480 Consumer Credit
<input type="checkbox"/> 190 Other Contract	<input checked="" type="checkbox"/> 360 Other Personal Injury	<input type="checkbox"/> 791 Employee Retirement Income Security Act	SOCIAL SECURITY	<input type="checkbox"/> 485 Telephone Consumer Protection Act
<input type="checkbox"/> 195 Contract Product Liability	<input type="checkbox"/> 362 Personal Injury -Medical Malpractice	IMMIGRATION	<input type="checkbox"/> 861 HIA (1395ff)	<input type="checkbox"/> 490 Cable/Sat TV
<input type="checkbox"/> 196 Franchise	CIVIL RIGHTS	<input type="checkbox"/> 462 Naturalization Application	<input type="checkbox"/> 862 Black Lung (923)	<input type="checkbox"/> 850 Securities/Commodities/Exchange
REAL PROPERTY	<input type="checkbox"/> 440 Other Civil Rights	<input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 863 DIWC/DIWW (405(g))	<input type="checkbox"/> 890 Other Statutory Actions
<input type="checkbox"/> 210 Land Condemnation	<input type="checkbox"/> 441 Voting		<input type="checkbox"/> 864 SSID Title XVI	<input type="checkbox"/> 891 Agricultural Acts
<input type="checkbox"/> 220 Foreclosure	<input type="checkbox"/> 442 Employment		<input type="checkbox"/> 865 RSI (405(g))	<input type="checkbox"/> 893 Environmental Matters
<input type="checkbox"/> 230 Rent Lease & Ejectment	<input type="checkbox"/> 443 Housing/Accommodations		<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant)	<input type="checkbox"/> 895 Freedom of Information Act
<input type="checkbox"/> 240 Torts to Land	<input type="checkbox"/> 445 Amer. w/Disabilities—Employment		<input type="checkbox"/> 871 IRS—Third Party 26 USC § 7609	<input type="checkbox"/> 896 Arbitration
<input type="checkbox"/> 245 Tort Product Liability	<input type="checkbox"/> 446 Amer. w/Disabilities—Other	OTHER		<input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision
<input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 448 Education	<input type="checkbox"/> 540 Mandamus & Other		<input type="checkbox"/> 950 Constitutionality of State Statutes
		<input type="checkbox"/> 550 Civil Rights		
		<input type="checkbox"/> 555 Prison Condition		
		<input type="checkbox"/> 560 Civil Detainee—Conditions of Confinement		

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

- | | | | | | | |
|---|---|--|---|--|--|---|
| <input checked="" type="checkbox"/> 1 Original Proceeding | <input type="checkbox"/> 2 Removed from State Court | <input type="checkbox"/> 3 Remanded from Appellate Court | <input type="checkbox"/> 4 Reinstated or Reopened | <input type="checkbox"/> 5 Transferred from Another District (specify) | <input type="checkbox"/> 6 Multidistrict Litigation—Transfer | <input type="checkbox"/> 8 Multidistrict Litigation—Direct File |
|---|---|--|---|--|--|---|

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):

Class Action Fairness Act, 28 U.S.C. § 1332(d)

Brief description of cause:

Negligence, California Consumer Privacy Act, Violations of California's Unfair Competition Law

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$

CHECK YES only if demanded in complaint:
JURY DEMAND: Yes No

VIII. RELATED CASE(S), IF ANY (See instructions):

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only)

SAN FRANCISCO/OAKLAND

SAN JOSE

EUREKA-MCKINLEYVILLE

DATE 02/04/2022

SIGNATURE OF ATTORNEY OF RECORD

/s/ M. Anderson Berry

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

- I. a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
- c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.