

1 Amy M. Hoffman (022762)
2 **THE WILKINS LAW FIRM, PLLC**
3 3300 N. Central Ave., Ste. 2600
4 Phoenix, AZ 85012
5 Tel: 602-795-0789
6 awilkins@wilkinslaw.net

7 Gayle M. Blatt*
8 *gmb@cglaw.com*
9 **CASEY GERRY SCHENK**
10 **FRANCAVILLA BLATT & PENFIELD, LLP**
11 110 Laurel Street
12 San Diego, CA 92101
13 Tel: (619) 238-1811; Fax: (619) 544-9232

14 *Pro Hac Vice Forthcoming
15
16 *Attorneys for Plaintiff and the*
17 *Putative Classes*

18 **IN THE UNITED STATES DISTRICT COURT**
19
20 **FOR THE DISTRICT OF ARIZONA**

21 Daniel Reed, on behalf of himself and
22 all other persons similarly situated,
23
24 Plaintiff,
25 v.
26 AmeriFirst Financial, Inc., an Arizona
27 corporation,
28 Defendant.

CASE NO.
CLASS ACTION COMPLAINT
Demand for Jury Trial

Plaintiff Daniel Reed, individually, and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby bring this Class Action Complaint against Defendant AmeriFirst Financial, Inc., and alleges as follows:

INTRODUCTION

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

1. Applicants for a loan must turn over valuable personal identifying information, including social security numbers, bank account numbers, driver’s license numbers, and addresses. If stolen, this highly sensitive information can be used by identity thieves to fraudulently open new accounts, access existing accounts, perpetrate identity fraud or impersonate victims in myriad schemes, all of which can cause grievous financial harm, negatively impact the victim’s credit scores for years, and cause victims to spend countless hours mitigating the impact.

2. Every year millions of Americans have their most valuable personal identifying information stolen and sold online because of data breaches. Despite the dire warnings about the severe impact of data breaches on Americans of all economic strata, companies still fail to put adequate security measures in place to protect their customers’ data.

3. Defendant AmeriFirst Financial, Inc. (“AmeriFirst”), an originator and provider of residential mortgage loans, is among those companies that have failed to meet their obligation to protect the sensitive personal identifying information (“PII”) entrusted to them by their customers.

4. For over a week, from about December 2, 2020 to December 10, 2020, an unknown third party gained unauthorized access to electronic data stored by AmeriFirst, including customer loan file information. The information stolen includes first and last names, Social Security numbers, driver’s licenses, bank account numbers, passport numbers, and other government-issued identification cards and numbers.

5. As a corporation doing business in Arizona, AmeriFirst is legally required to secure the PII it collects by implementing reasonable and appropriate data security safeguards and protecting PII from unauthorized access.

6. As a result of AmeriFirst’s failure to provide adequate data security,

1 Plaintiff's and the Class¹ members' PII has been exposed to those who should not
2 have access to it. Plaintiff and the Class have suffered the damages alleged below
3 and are now at much higher risk of identity theft and for cybercrimes of all kinds.

4 **THE PARTIES**

5 7. Defendant AmeriFirst, Inc., is an Arizona corporation with its principal
6 place of business in Gilbert, Arizona. AmeriFirst is an originator and provider of
7 residential mortgage loans with locations in Arizona and across the nation. With
8 over 70 locations across the country and over 700 employees, including around 250
9 licensed loan consultants, AmeriFirst's estimated annual revenues exceed \$78
10 million.

11 8. Plaintiff Daniel Reed is a resident of Goodyear, Arizona. On or about
12 April 21, 2021, Plaintiff Reed received notice from AmeriFirst that it improperly
13 exposed his PII to unauthorized third parties. In or about 2012, Plaintiff Reed
14 provided his PII to Defendant to obtain a home mortgage loan.

15 9. Plaintiff reasonably believed AmeriFirst would keep his PII secure, and
16 only for the time period for which it was required to be maintained. Had
17 AmeriFirst disclosed to Plaintiff that his PII would not be kept secure and would
18 be kept easily accessible to hacker and third parties, including long after it was
19 necessary for their business purpose, he would have taken additional precautions
20 relating to his PII or not provided it to Defendant, and instead sought to do
21 business with another home mortgage lender.

22 **JURISDICTION AND VENUE**

23 10. Subject matter jurisdiction in this civil action is authorized pursuant to
24 28 U.S.C. § 1332(d) because there are more than 100 Class members, at least one
25 class member is a citizen of a state different from that of Defendant, and the
26

27 ¹ As used herein, the "Class" means the putative National Class and Arizona
28 Subclass defined below.

1 amount in controversy exceeds \$5 million, exclusive of interest and costs. This
2 Court has supplemental jurisdiction over the state law claims pursuant to 18
3 U.S.C. § 1367.

4 11. This Court has personal jurisdiction over Defendant because it is an
5 Arizona corporation and maintains its principal place of business in this District,
6 and intentionally avails itself of consumers and markets within this District, so it
7 has sufficient minimum contacts with this District.

8 12. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because
9 Defendant resides in this District and a substantial part of the events or omissions
10 giving rise to Plaintiff's and Class members' claims occurred in this District.

11 13. Application of Arizona law to this dispute is proper because
12 Defendant's headquarters are in Arizona, the decisions or actions that gave rise to
13 the underlying facts at issue in this Complaint were presumably made or taken in
14 Arizona, and the action and/or inaction at issue emanated from Arizona.

15 **FACTUAL ALLEGATIONS**

16 **A. AmeriFirst collects and stores customers' PII and fails to provide**
17 **adequate data security.**

18 14. AmeriFirst employs over 700 people, including around 250 licensed
19 loan consultants in over 70 locations across the country. Its annual revenue
20 exceeds \$78 million.

21 15. AmeriFirst provides a full range of home loans including conventional,
22 FHA, VA, USDA Rural Development, FHA Standard and Limited 203(k) Home
23 Improvement loans.

24 16. On December 2, 2020 and continuing through on or about December 10,
25 2020, an unknown third party gained access to AmeriFirst's electronic data storage
26 system that was used to store customer data, resulting in customers' PII being
27 exposed.

28 17. Customers' names, social security numbers, driver's license numbers,

1 bank account numbers, passport numbers, and “other government issued
2 identification card and numbers” were among the PII that was compromised and
3 stolen by the unauthorized party or parties.

4 18. This incident is referred to herein as the “Data Breach.”

5 19. Plaintiff received a letter titled “Notice of Data Breach,” dated April 15,
6 2021, from AmeriFirst. The letter stated that their PII, including those mentioned
7 above, may have been compromised, and included the following:

8 **What Happened?**

9 On or about April 12, 2021, AmeriFirst Financial, Inc. (“AmeriFirst”)
10 ascertained that our electronic data storage of certain customers’ loan
11 file information was compromised, which resulted in the exposure of
12 your personal information. It appears that the exposure began on or
about December 2, 2020, and ended on or about December 10, 2020.

13 **What Information Was Involved?**

14 The personal information about certain AmeriFirst’s customers
15 affected by the exposure included first and last names; Social Security
16 numbers; bank account numbers; driver’s license; passport numbers;
17 and other government issues identification cards and numbers.²

18 20. In addition, AmeriFirst filed a “Data Breach Notifications” form with
19 the Office of the Maine Attorney General in which it disclosed that the “[t]otal
20 number of persons affected” by the Data Breach is 103,607.³
21
22
23
24
25

26
27 ² AmeriFirst’s “Notice of Data Breach” sent to Plaintiff on April 15, 2021.

28 ³ <https://apps.web.maine.gov/online/aeviewer/ME/40/855b0dda-679e-4353-bfca-4098ce9b303f.shtml>

1 **B. The PII exposed by AmeriFirst as a result of its inadequate data security**
2 **is highly valuable on the black market.**

3 21. The information exposed by AmeriFirst is a virtual goldmine for
4 phishers, hackers, identity thieves and cyber criminals.

5 22. This exposure is tremendously problematic. Cybercrime is rising at an
6 exponential rate.

7 23. According to experts, one out of four data breach notification recipients
8 become a victim of identity fraud.

9 24. Stolen PII is often trafficked on the “dark web,” a heavily encrypted
10 part of the Internet that is not accessible via traditional search engines. Law
11 enforcement has difficulty policing the “dark web” due to this encryption, which
12 allows users and criminals to conceal identities and online activity.

13 25. The PII of consumers remains of high value to criminals, as evidenced
14 by the prices they will pay through the dark web. Numerous sources cite dark web
15 pricing for stolen identity credentials. For example, personal information can be
16 sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50
17 to \$200⁴. Experian reports that a stolen credit or debit card number can sell for \$5
18 to \$110 on the dark web.⁵

19 26. Social Security numbers, for example, are among the worst kind of
20 personal information to have stolen because they may be put to a variety of
21 fraudulent uses and are difficult for an individual to change. The Social Security
22

23 ⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital
24 Trends, Oct. 16, 2019, available at:
25 [https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-
web-how-much-it-costs/](https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/) (last accessed Nov. 11, 2020).

26 ⁵ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian,
27 Dec. 6, 2017, available at: [https://www.experian.com/blogs/ask-experian/heres-
how-much-your-personal-information-is-selling-for-on-the-dark-web/](https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/) (last
28 accessed Nov. 11, 2020).

1 Administration stresses that the loss of an individual's Social Security number, as
2 is the case here, can lead to identity theft and extensive financial fraud:

3 A dishonest person who has your Social Security number can use
4 it to get other personal information about you. Identity thieves can
5 use your number and your good credit to apply for more credit in
6 your name. Then, they use the credit cards and don't pay the bills,
7 it damages your credit. You may not find out that someone is
8 using your number until you're turned down for credit, or you
9 begin to get calls from unknown creditors demanding payment for
items you never bought. Someone illegally using your Social
Security number and assuming your identity can cause a lot of
problems⁶.

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

16 28. Even then, a new Social Security number may not be effective.
17 According to Julie Ferguson of the Identity Theft Resource Center, "The credit
18 bureaus and banks are able to link the new number very quickly to the old
19 number, so all of that old bad information is quickly inherited into the new Social
20 Security number."⁷

21 29. Because of this, the information compromised in the Data Breach here is
22 significantly more valuable than the loss of, for example, credit card information in
23

24 ⁶ Social Security Administration, *Identity Theft and Your Social Security Number*,
25 available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 11,
2020).

26 ⁷ Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*,
27 NPR (Feb. 9, 2015), available at:
28 [http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-
has-millionsworrying-about-identity-theft](http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft) (last visited Nov. 11, 2020).

1 a retailer data breach because, there, victims can cancel or close credit and debit
2 card accounts. The information compromised in this Data Breach is impossible to
3 “close” and difficult, if not impossible, to change – Social Security number, driver’s
4 license number, bank information, passport number, name, date of birth, and
5 addresses.

6 30. This data demands a much higher price on the black market. Martin
7 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to
8 credit card information, personally identifiable information and Social Security
9 numbers are worth more than 10 times on the black market.”⁸

10 31. Once PII is sold, it is often used to gain access to various areas of the
11 victim’s digital life, including bank accounts, social media, credit card, and tax
12 details. This can lead to additional PII being harvested from the victim, as well as
13 PII from family, friends and colleagues of the original victim.

14 32. According to the FBI’s Internet Crime Complaint Center (IC3) 2019
15 Internet Crime Report, Internet-enabled crimes reached their highest number of
16 complaints and dollar losses in 2019, resulting in more than \$3.5 billion in losses to
17 individuals and business victims.

18 33. Further, according to the same report, “rapid reporting can help law
19 enforcement stop fraudulent transactions before a victim loses the money for
20 good.” Defendant did not rapidly report to Plaintiff and Class members that their
21 PII had been stolen. It took Defendant almost five months to notify them.

22 34. Victims of identity theft also often suffer embarrassment, blackmail, or
23 harassment in person or online, and/or experience financial losses resulting from
24

25 ⁸ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit*
26 *Card Numbers*, IT World, (Feb. 6, 2015), available at:
27 [https://www.networkworld.com/article/2880366/anthem-hack-personal-data-](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)
28 [stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last visited Nov. 11,
2020).

1 fraudulently opened accounts or misuse of existing accounts.

2 35. Data breaches facilitate identity theft as hackers obtain consumers' PII
3 and thereafter use it to siphon money from current accounts, open new accounts in
4 the names of their victims, or sell consumers' PII to others who do the same.

5 36. For example, The United States Government Accountability Office
6 noted in a June 2007 report on data breaches (the "GAO Report") that criminals
7 use PII to open financial accounts, receive government benefits, and make
8 purchases and secure credit in a victim's name.⁹ The GAO Report further notes
9 that this type of identity fraud is the most harmful because it may take some time
10 for a victim to become aware of the fraud, and can adversely impact the victim's
11 credit rating in the meantime. The GAO Report also states that identity theft
12 victims will face "substantial costs and inconveniences repairing damage to their
13 credit records . . . [and their] good name."¹⁰

14 **C. AmeriFirst Failed to Comply with Federal Trade Commission**
15 **Requirements**

16 37. Federal and State governments have established security standards and
17 issued recommendations to minimize data breaches and the resulting harm to
18 individuals and financial institutions. The Federal Trade Commission ("FTC") has
19 issued numerous guides for businesses that highlight the importance of reasonable
20 data security practices. According to the FTC, the need for data security should be
21 factored into all business decision-making.¹¹

23 ⁹ See Government Accountability Office, *Personal Information: Data Breaches are*
24 *Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is*
25 *Unknown* (June 2007), available at <http://www.gao.gov/assets/270/262899.pdf>
(last visited October 6, 2020).

26 ¹⁰ *Id.*

27 ¹¹ See Federal Trade Commission, *Start With Security* (June 2015),
28 [https://www.ftc.gov/system/files/documents/plain-language/pdf0205-
startwithsecurity.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf) (last visited October 6, 2020).

1 38. In 2016, the FTC updated its publication, *Protecting Personal Information:*
2 *A Guide for Business*, which established guidelines for fundamental data security
3 principles and practices for business.¹² Among other things, the guidelines note
4 businesses should properly dispose of personal information that is no longer
5 needed; encrypt information stored on computer networks; understand their
6 network's vulnerabilities; and implement policies to correct security problems. The
7 guidelines also recommend that businesses use an intrusion detection system to
8 expose a breach as soon as it occurs; monitor all incoming traffic for activity
9 indicating someone is attempting to hack the system; watch for large amounts of
10 data being transmitted from the system; and have a response plan ready in the
11 event of a breach.¹³

12 39. Additionally, the FTC recommends that companies limit access to
13 sensitive data; require complex passwords to be used on networks; use industry-
14 tested methods for security; monitor for suspicious activity on the network; and
15 verify that third-party service providers have implemented reasonable security
16 measures.¹⁴

17 40. Highlighting the importance of protecting against data breaches, the
18 FTC has brought enforcement actions against businesses for failing to adequately
19 and reasonably protect PII, treating the failure to employ reasonable and
20 appropriate measures to protect against unauthorized access to confidential
21 consumer data as an unfair act or practice prohibited by Section 5 of the Federal
22 Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these
23 actions further clarify the measures businesses must take to meet their data
24

25
26 ¹² See Federal Trade Commission, *Protecting Personal Information: A Guide for*
27 *Business* (Oct. 2016), [https://www.ftc.gov/system/files/documents/plain-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
28 [language/pdf-0136_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last October 6, 2020).

¹³ *Id.*

¹⁴ Federal Trade Commission, *Start With Security*, *supra* note 5.

1 security obligations.¹⁵

2 41. By allowing an unknown third party to access AmeriFirst's data storage
3 system and expose customers' PII, AmeriFirst failed to employ reasonable and
4 appropriate measures to protect against unauthorized access to confidential
5 customer data, and as a result, allowed an unknown third party to access its data
6 storage system and expose customers' PII. AmeriFirst's data security policies and
7 practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act,
8 15 U.S.C. § 45.

9 **D. Plaintiff engaged in measures to attempt to secure his PII after the**
10 **breach.**

11 42. Upon receiving Notice from AmeriFirst on or about April 21, 2021,
12 Plaintiff researched his options to respond to the theft of his name and Social
13 Security Number. He spent and will continue to spend additional time reviewing
14 his financial accounts for fraudulent activity. This is time Plaintiff otherwise
15 would have spent performing other activities, such as his job and/or leisurely
16 activities for the enjoyment of life.

17 43. Plaintiff suffered actual injury from having his PII exposed as a result of
18 the Data Breach including, but not limited to: (a) damages to and diminution in the
19 value of his PII—a form of intangible property that Plaintiff entrusted to
20 AmeriFirst as a condition of applying for and receiving a home loan; (b) loss of his
21 privacy; and (c) imminent and impending injury arising from the increased risk of
22 fraud and identity theft.

23 44. As a result of the Data Breach, Plaintiff will continue to be at
24 heightened risk for financial fraud, identity theft, other forms of fraud, and the
25 attendant damages, for years to come.

26
27 ¹⁵ Federal Trade Commission, *Privacy and Security Enforcement Press Releases*,
28 <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement> (last visited October 6, 2020).

1 **E. Plaintiff and the Class members suffered damages.**

2 45. The ramifications of Defendant's failure to keep customers' PII secure
3 are long lasting and severe. Once PII is stolen, fraudulent use of that information
4 and damage to victims may continue for years.¹⁶

5 46. The PII belonging to Plaintiff and Class members is private, sensitive in
6 nature, and was inadequately protected by Defendant who did not obtain
7 Plaintiff's or Class members' consent to disclose such PII to any other person as
8 required by applicable law and industry standards.

9 47. The Data Breach was a direct and proximate result of AmeriFirst's
10 failure to: (a) properly safeguard and protect Plaintiff's and Class members' PII
11 from unauthorized access, use, and disclosure, as required by various state and
12 federal regulations, industry practices, and common law; (b) establish and
13 implement appropriate administrative, technical, and physical safeguards to
14 ensure the security and confidentiality of Plaintiff's and Class members' PII; and
15 (c) protect against reasonably foreseeable threats to the security or integrity of such
16 information.

17 48. Defendant had the resources necessary to prevent the Data Breach, but
18 neglected to adequately implement data security measures, despite its obligation
19 to protect customers' PII.

20 49. Had Defendant remedied the deficiencies in its data security systems
21 and adopted security measures recommended by experts in the field, it would
22 have prevented the intrusions into its systems and, ultimately, the theft of PII.

23 50. As a direct and proximate result of Defendant's wrongful actions and
24 inactions, Plaintiff and Class members have been placed at an imminent,
25

26
27 ¹⁶ 2014 LexisNexis True Cost of Fraud Study, available at:
28 <https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf>
(last accessed Nov. 11, 2020).

1 immediate, and continuing increased risk of harm from identity theft and fraud,
2 requiring them to take the time which they otherwise would have dedicated to
3 other life demands such as work and family in an effort to mitigate the actual and
4 potential impact of the Data Breach on their lives.

5 51. The U.S. Department of Justice's Bureau of Justice Statistics found that
6 "among victims who had personal information used for fraudulent purposes, 29%
7 spent a month or more resolving problems" and that "resolving the problems
8 caused by identity theft [could] take more than a year for some victims."¹⁷

9 52. As a result of the Defendant's failures to prevent the Data Breach,
10 Plaintiff and Class members have suffered, will suffer, and are at increased risk of
11 suffering:

- 12 a. The compromise, publication, theft, and/or unauthorized use of their
13 PII;
- 14 b. Out-of-pocket costs associated with the prevention, detection, recovery,
15 and remediation from identity theft or fraud;
- 16 c. Lost opportunity costs and lost wages associated with efforts expended
17 and the loss of productivity from addressing and attempting to mitigate
18 the actual and future consequences of the Data Breach, including but not
19 limited to efforts spent researching how to prevent, detect, contest, and
20 recover from identity theft and fraud;
- 21 d. The continued risk to their PII, which remains in the possession of
22 Defendant and is subject to further breaches so long as Defendant fails
23 to undertake appropriate measures to protect the PII in its possession;
24 and

25
26
27 ¹⁷ U.S. Department of Justice, Office of Justice Programs Bureau of Justice
28 Statistics, *Victims of Identity Theft*, 2012, December 2013, available at:
<https://www.bjs.gov/content/pub/pdf/vit12.pdf> (last accessed Nov. 11, 2020).

1 e. Current and future costs in terms of time, effort, and money that will be
2 expended to prevent, detect, contest, remediate, and repair the impact of
3 the Data Breach for the remainder of the lives of Plaintiff and Class
4 members.

5 53. In addition to a remedy for the economic harm, Plaintiff and Class
6 members maintain an undeniable interest in ensuring that their PII is secure,
7 remains secure, and is not subject to further misappropriation and theft.

8 54. To date, other than providing 1 year of identity monitoring services,
9 Defendant does not appear to be taking any measures to assist Plaintiff and Class
10 members.

11 55. Defendant's offer of 1 year of identity monitoring services is woefully
12 inadequate. While some harm has begun already, the worst may be yet to come.
13 There may be a time lag between when harm occurs versus when it is discovered,
14 and also between when PII is acquired and when it is used. Furthermore, identity
15 theft monitoring services only alert someone to the fact that they have already
16 been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another
17 person's PII) – they do not prevent identity theft.

18 **F. AmeriFirst's delay in identifying and reporting the breach caused**
19 **additional harm.**

20 56. Although their PII was improperly exposed in or about December 2020,
21 Plaintiff and the Class were not notified of the Data Breach until four months later,
22 on or about April 15, 2021, depriving them of the ability to promptly mitigate
23 potential adverse consequences resulting from the Data Breach.

24 57. As a result of AmeriFirst's delay in detecting and notifying customers
25 of the Data Breach, the risk of fraud has been driven even higher.

26 **CHOICE OF LAW**

27 58. Defendant is headquartered in Arizona. Upon information and belief,
28 Arizona is the nerve center of Defendant's business activities – the place where

1 high-level officers direct, control, and coordinate Defendant's activities, including
2 data security, and where: (a) major policy; (b) advertising; and (c) financial and
3 legal decisions originate.

4 59. Further, upon information and belief, Data security assessments and
5 other IT duties related to computer systems and data security occur at Defendant's
6 Arizona headquarters. Furthermore, Defendant's response, and corporate
7 decisions surrounding such response, to the Data Breach were made from and in
8 Arizona. Finally, Defendant's breach of its duty to customers – including Plaintiff
9 and Class and Subclass members, emanated from Arizona and thus, Defendant
10 cannot claim to be surprised by application of Arizona law to regulate its conduct.

11 60. To the extent Arizona law conflicts with the law of any other state that
12 could apply to Plaintiff's claims against Defendant, application of Arizona law
13 would lead to the most predictable result, promote the maintenance of interstate
14 order, simplify the judicial task, and advance the forum's governmental interest.

15 CLASS ACTION ALLEGATIONS

16 61. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff
17 brings this action on behalf of himself and the following proposed Nationwide
18 Class, defined as follows:

19 All persons residing in the United States who are customers of
20 AmeriFirst or any affiliate, parent, or subsidiary of AmeriFirst who
21 had their PII compromised as a result of the Data Breach that
22 occurred from December 2, 2020 to December 10, 2020.

23 In addition, Plaintiff brings this action on behalf of himself and the
24 following proposed Arizona subclass defined as follows:

25 All persons residing in the State of Arizona who are customers of
26 AmeriFirst or any affiliate, parent, or subsidiary of AmeriFirst who
27 had their PII compromised as a result of the Data Breach that
28 occurred from December 2, 2020 to December 10, 2020.

62. Both the proposed National Class and the proposed Arizona subclass

1 will be collectively referred to as the Class except where it is necessary to
2 differentiate them.

3 63. Excluded from the proposed Class are any officer or director of
4 Defendant; any officer or director of any affiliate, parent, or subsidiary of
5 AmeriFirst; anyone employed by counsel in this action; and any judge to whom
6 this case is assigned, his or her spouse, and members of the judge's staff.

7 64. **Numerosity.** Members of the proposed Class likely number in the
8 thousands and are thus too numerous to practically join in a single action.
9 Membership in the Class is readily ascertainable from Defendant's own records.

10 65. **Commonality and Predominance.** Common questions of law and fact
11 exist as to all proposed Class members and predominate over questions affecting
12 only individual Class members. These common questions include:

- 13 a. Whether Defendant engaged in the wrongful conduct alleged herein;
- 14 b. Whether Defendant's inadequate data security measures were a cause of the
15 data security breach;
- 16 c. Whether Defendant owed a legal duty to Plaintiff and the other Class
17 members to exercise due care in collecting, storing, and safeguarding their PII;
- 18 d. Whether Defendant negligently or recklessly breached legal duties owed to
19 Plaintiff and the other Class members to exercise due care in collecting,
20 storing, and safeguarding their PII;
- 21 e. Whether Plaintiff and the Class are at an increased risk for identity theft
22 because of the data security breach;
- 23 f. Whether Defendant failed to provide timely notice of the Data Breach to
24 Plaintiff and Class members;
- 25 g. Whether Plaintiff and the other Class members are entitled to actual,
26 statutory, or other forms of damages, and other monetary relief; and
- 27 h. Whether Plaintiff and the other Class members are entitled to equitable relief,
28 including, but not limited to, injunctive relief and restitution.

1 66. Defendant engaged in a common course of conduct giving rise to the
2 legal rights sought to be enforced by Plaintiff individually and on behalf of the
3 other Class members. Similar or identical statutory and common law violations,
4 business practices, and injuries are involved. Individual questions, if any, pale by
5 comparison, in both quantity and quality, to the numerous common questions that
6 dominate this action.

7 67. **Typicality:** Plaintiff's claims are typical of the claims of the members of
8 the Class. All Class members were subject to the Data Breach and had their PII
9 accessed by and/or disclosed to unauthorized third parties. Defendant's
10 misconduct impacted all Class members in the same manner.

11 68. **Adequacy of Representation:** Plaintiff is an adequate representative of
12 the Class because his interests do not conflict with the interests of the other Class
13 members he seeks to represent; he has retained counsel competent and
14 experienced in complex class action litigation, and Plaintiff will prosecute this
15 action vigorously. The interests of the Class will be fairly and adequately protected
16 by Plaintiff and his counsel.

17 69. **Superiority:** A class action is superior to any other available means for
18 the fair and efficient adjudication of this controversy, and no unusual difficulties
19 are likely to be encountered in the management of this matter as a class action. The
20 damages, harm, or other financial detriment suffered individually by Plaintiff and
21 the other Class members are relatively small compared to the burden and expense
22 that would be required to litigate their claims on an individual basis against
23 Defendant, making it impracticable for Class members to individually seek redress
24 for Defendant's wrongful conduct. Individualized litigation would create a
25 potential for inconsistent or contradictory judgments and increase the delay and
26 expense to all parties and the court system. By contrast, the class action device
27 presents far fewer management difficulties and provides the benefits of single
28 adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Negligence

(On behalf of Plaintiff and the National Class and Arizona Subclass)

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

70. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

71. Defendant required Plaintiff and Class members to submit sensitive personal and financial information in order to obtain its services.

72. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class members' PII from being compromised, lost, stolen, and accessed by unauthorized persons. This duty includes, among other things, designing, maintaining, and testing its data security systems to ensure that Plaintiff's and Class members' PII in Defendant's possession was adequately secured and protected.

73. Defendant owed a duty of care to Plaintiff and Class members to provide security, consistent with industry standards, to ensure that its systems and networks adequately protected the PII of its customers.

74. Plaintiff and Class members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information, and Defendant was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

75. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Defendant's misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Data Breach.

76. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and the importance of adequate security. Defendant knew about - or should have been aware of - numerous, well-publicized data

1 breaches affecting businesses in the United States.

2 77. Defendant breached its duties to Plaintiff and Class members by failing
3 to provide fair, reasonable, or adequate computer systems and data security to
4 safeguard the PII of Plaintiff and Class members.

5 78. Because Defendant knew that a breach of its systems would damage
6 thousands of current and former AmeriFirst customers, including Plaintiff and
7 Class members, Defendant had a duty to adequately protect its data systems and
8 the PII contained therein.

9 79. Defendant had a special relationship with Plaintiff and Class members
10 by virtue of providing them mortgage services. Plaintiff and Class members
11 reasonably believed that Defendant would take adequate security precautions to
12 protect their PII.

13 80. As a result of Defendant's failure to exercise reasonable care as
14 identified above, Plaintiff and Class members were harmed, and Defendant's
15 actions and omissions are a proximate cause of their injuries and damages.

16 **SECOND CAUSE OF ACTION**

17 ***Negligence Per Se***

18 **(On behalf of Plaintiff and the National Class and Arizona Subclass)**

19 81. Plaintiff incorporates by reference all previous allegations as though
20 fully set forth herein.

21 82. Pursuant to Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendant had
22 a duty to protect the security and confidentiality of Plaintiff's and Class Members'
23 personal information.

24 83. Defendant breached its duties to Plaintiff and Class members under the
25 Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate data
26 security practices to safeguard Plaintiff's and Class members' personal
27 information.

28 84. Defendant's failure to comply with applicable laws and regulations

1 constitutes negligence *per se*.

2 85. But for Defendant's wrongful and negligent breach of its duties owed
3 to Plaintiff and Class members, they would not have been injured.

4 86. The injury and harm suffered by Plaintiff and Class members was the
5 reasonably foreseeable result of Defendant's breach of its duties. Defendant knew
6 or should have known that it was failing to meet its duties, and that its breach
7 would cause Plaintiff and Class Members to experience the foreseeable harms
8 associated with the exposure of their PII.

9 87. As a direct and proximate result of Defendant's negligent conduct,
10 Plaintiff and Class members have suffered injury and are entitled to damages in an
11 amount to be proven at trial.

12 **THIRD CAUSE OF ACTION**

13 **Unjust Enrichment**

14 **(On behalf of Plaintiff and the National Class and Arizona Subclass)**

15 88. Plaintiff incorporates by reference all previous allegations as though
16 fully set forth herein.

17 89. Plaintiff and Class members conferred a monetary benefit on
18 Defendant. Specifically, they provided their PII to Defendant which Defendant
19 then used to extend residential home loans to them at a profit to Defendant. In
20 exchange, Plaintiff and Class members should have at a minimum had their PII
21 protected with adequate data security measures.

22 90. Defendant knew that Plaintiff and Class members conferred a benefit
23 that Defendant accepted. Defendant profited from these transactions and used the
24 PII of Plaintiff and Class members for business purposes.

25 91. The monies that Defendant profited from Plaintiff's and Class
26 members' providing their PII for home loans was used, in part, to pay for use of
27 Defendant's network and the administrative costs of data management and
28

1 security.

2 92. Under the principles of equity and good conscience, Defendant should
3 not be permitted to retain the money belonging to Plaintiff and Class members or
4 the money it made via its extending home loans to Plaintiff and Class members,
5 because Defendant failed to implement appropriate data management and
6 security measures that are mandated by statutory and common law as well as
7 industry standards.

8 93. Defendant failed to secure Plaintiff's and Class members' PII and,
9 therefore, did not provide full benefit for the value Plaintiff and Class members
10 provided.

11 94. Defendant acquired the PII through inequitable means in that it failed
12 to disclose the inadequate security practices previously alleged.

13 95. If Plaintiff and Class members knew that Defendant had not reasonably
14 secured their PII, they would not have provided their PII to Defendant, or they
15 would not have given Defendant their PII on the same terms.

16 96. Plaintiff and Class members have no adequate remedy at law.

17 97. As a direct and proximate result of Defendant's conduct, Plaintiff and
18 Class members have suffered and will continue to suffer other forms of injury
19 and/or harm, including a substantial and imminent risk of identity theft.

20 98. Defendant should be compelled to disgorge into a common fund or
21 constructive trust, for the benefit of Plaintiff and Class members, proceeds that it
22 unjustly received from Plaintiff and Class members or that it unjustly received by
23 doing business with Plaintiff and Class members.

24 **PRAYER FOR RELIEF**

25 WHEREFORE, Plaintiff, individually, and on behalf of all others similarly
26 situated, respectfully requests that the Court enter an order:

- 27 a. Certifying the proposed National Class and Arizona Subclass as requested
28 herein;

1 b. Appointing Plaintiff as Class Representative and undersigned counsel as Class
2 Counsel;

3 c. Finding that Defendant engaged in the unlawful conduct as alleged herein;

4 d. Awarding Plaintiff and the Class appropriate monetary relief, including actual
5 damages, restitution, and disgorgement.

6 e. Awarding Plaintiff and Class members pre-judgment and post-judgment
7 interest on all amounts awarded;

8 f. Awarding Plaintiff and the Class equitable, injunctive and declaratory relief as
9 may be appropriate. Plaintiff, on behalf of the Class, seeks appropriate
10 injunctive relief designed to ensure against the recurrence of a data breach by
11 adopting and implementing best security data practices to safeguard
12 Defendant’s customers’ financial, and personal information that would
13 include, without limitation an order and judgment directing Defendant to:

14 (i) protect all data collected or received through the course
15 of its business in accordance with federal, state and
16 local laws, and best practices under industry standards;

17 (ii) requiring Defendant to design, maintain, and test its
18 computer systems to ensure that PII in its possession is
19 adequately secured and protected;

20 (iii) requiring Defendant to disclose any future data
21 breaches in a timely and accurate manner;

22 (iv) requiring Defendant to engage third-party security
23 auditors as well as internal security personnel to
24 conduct testing, including simulated attacks,
25 penetration tests, and audits on Defendant’s systems on
26 a periodic basis and ordering it to promptly correct any
27 problems or issues detected by these auditors;

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

- (v) requiring Defendant to audit, test, and train its security personnel to run automated security monitoring, aggregating, filtering and reporting on log information in a unified manner;
- (vi) requiring Defendant to implement multi-factor authentication requirements;
- (vii) requiring Defendant’s employees to change their passwords on a timely and regular basis, consistent with best practices;
- (viii) requiring Defendant to encrypt all PII;
- (ix) (requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- (x) requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant’s network is compromised, hackers cannot gain access to other portions of Defendant’s systems;
- (xi) requiring Defendant to purge, delete, and destroy in a reasonably secure and timely manner PII no longer necessary for the provision of services;
- (xii) requiring Defendant to conduct regular computer system scanning and security checks;
- (xiii) requiring Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

(xiv) requiring Defendant to provide lifetime credit monitoring and identity theft repair services to Class members; and

(xv) requiring Defendant to educate all Class members about the threats they face as a result of the loss of their PII to third parties, as well as steps Class members must take to protect themselves

g. Awarding Plaintiff and the Class members reasonable attorneys’ fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Classes, hereby demands a trial by jury as to all matters so triable.

Dated: April 26, 2021

THE WILKINS LAW FIRM, PLLC

/s/ Amy M. Hoffman
Amy M. Hoffman
awilkins@wilkinslaw.net
3300 N. Central Ave., Ste. 2600
Phoenix, AZ 85012
Tel: 602-795-0789

CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD, LLP
Gayle M. Blatt
gmb@cglaw.com
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232

Attorneys for Plaintiff and the putative Class

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

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): Daniel Reed

Defendant(s): AmeriFirst Financial, Inc

County of Residence: Maricopa

County of Residence: Maricopa

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Defendant's Atty(s):

**Amy M Hoffman , Attorney
The Wilkins Law Firm
3300 N. Central Avenue, Suite 2600
Phoenix, Arizona 85012
602-795-0789**

II. Basis of Jurisdiction:

3. Federal Question (U.S. not a party)

III. Citizenship of Principal Parties (Diversity Cases Only)

Plaintiff:- N/A

Defendant:- N/A

IV. Origin :

1. Original Proceeding

V. Nature of Suit:

190 Other Contract

VI. Cause of Action:

Data Security breach pursuant to Rule 23 of the Federal Rules of Civil Procedure; Arizona subclass Gramm-Leach-Bliley Act (15 U.S.C. § 6801)

VII. Requested in Complaint

Class Action: **Yes**

Dollar Demand: **Exceeds \$5 Million**

Jury Demand: **Yes**

VIII. This case is not related to another case.

Signature: Amy M. Hoffman

Date: 4/26/2021

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Class Action Filed Over December 2020 AmeriFirst Data Breach](#)
