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

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

*Pro Hac Vice Forthcoming

Attorneys for Plaintiff and the Putative Classes

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Daniel Reed, on behalf of himself and all other persons similarly situated, Plaintiff, v. AmeriFirst Financial, Inc., an Arizona corporation, 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. 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,

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

THE PARTIES

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

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

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

JURISDICTION AND VENUE

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

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

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

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

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

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

FACTUAL ALLEGATIONS

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

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

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

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

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

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

18. This incident is referred to herein as the "Data Breach."

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

> **What Happened?**
>
> On or about April 12, 2021, AmeriFirst Financial, Inc. ("AmeriFirst") ascertained that our electronic data storage of certain customers' loan file information was compromised, which resulted in the exposure of your personal information. It appears that the exposure began on or about December 2, 2020, and ended on or about December 10, 2020.
>
> **What Information Was Involved?**
>
> The personal information about certain AmeriFirst's customers affected by the exposure included first and last names; Social Security numbers; bank account numbers; driver's license; passport numbers; and other government issues identification cards and numbers.[2]

20. In addition, AmeriFirst filed a "Data Breach Notifications" form with the Office of the Maine Attorney General in which it disclosed that the "[t]otal number of persons affected" by the Data Breach is 103,607.[3]

[2] AmeriFirst's "Notice of Data Breach" sent to Plaintiff on April 15, 2021.
[3] https://apps.web.maine.gov/online/aeviewer/ME/40/855b0dda-679e-4353-bfca-4098ce9b303f.shtml

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

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

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

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

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

25. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[4]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[5]

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

---

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

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

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

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

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

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

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

---

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

[7] 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 Nov. 11, 2020).

a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security number, driver's license number, bank information, passport number, name, date of birth, and addresses.

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

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

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

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

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

---

[8] 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 Nov. 11, 2020).

fraudulently opened accounts or misuse of existing accounts.

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

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

C. AmeriFirst Failed to Comply with Federal Trade Commission Requirements

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

---

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

[10] *Id.*

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

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

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

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

---

[12] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), 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.

security obligations.[15]

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

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

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

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

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

---

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

E. Plaintiff and the Class members suffered damages.

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

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

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

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

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

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

---

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

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

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

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

a. The compromise, publication, theft, and/or unauthorized use of their PII;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their PII, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII in its possession; and

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

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

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

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

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

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

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

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

CHOICE OF LAW

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

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

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

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

CLASS ACTION ALLEGATIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

breaches affecting businesses in the United States.

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

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

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

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

SECOND CAUSE OF ACTION

Negligence *Per Se*

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

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

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

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

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

constitutes negligence *per se.*

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

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

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

THIRD CAUSE OF ACTION

Unjust Enrichment

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

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

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

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

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

security.

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

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

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

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

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

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

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

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

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

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

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

(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;

(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