IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

DOROTHY ZELENSKI, individually and on behalf of all others similarly situated, Plaintiff, v. AMERICAN FINANCIAL RESOURCES, INC. Defendant.	**Case No.:** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Dorothy Zelenski ("Plaintiff Zelenski"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant American Financial Resources, Inc. ("AFR" or "Defendant"). Facts pertaining to Plaintiff and her personal experiences and circumstances are alleged based upon personal knowledge and all other facts herein are alleged based upon information and belief, *inter alia*, the investigation of Plaintiff's counsel.

NATURE OF THE ACTION

1. This is a class action for damages with respect to American Financial Resources, Inc. for its failure to exercise reasonable care in securing and safeguarding its client's sensitive information—including names, Social Security Numbers, and drivers' license numbers (the "PII" or "Private Information").

2. This class action is brought on behalf of customers who used AFR's services and had their sensitive PII accessed by unauthorized parties because of a lapse in network security in or around December of 2021 (the "Data Breach").

3. The Data Breach affected customers who use AFR's services in multiple states.

4. AFR reported to Plaintiff that information compromised in the Data Breach included her PII.

5. Plaintiff was not notified of the Data Breach until mid-March of 2022, approximately three months after her information was first accessed.

6. As a result of the Data Breach, Plaintiff and Class members will experience various types of misuse of their PII in the coming years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their financial information.

7. There has been no assurance offered from AFR that all personal data or copies of data have been recovered or destroyed. AFR offered Kroll identity monitoring, which does not guarantee the security of Plaintiff's information. To mitigate further harm, Plaintiff chose not to disclose any more information to receive these services connected with AFR.

8. Accordingly, Plaintiff asserts claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, bailment, unjust enrichment, breach of confidence, violations of New Jersey and Pennsylvania consumer protection statutes, and declaratory and injunctive relief.

PARTIES

A. Plaintiff Dorothy Zelenski

9. Plaintiff Dorothy Zelenski is a resident of Bensalem, Pennsylvania, and brings this action in her individual capacity and on behalf of all others similarly situated. Plaintiff Zelenski's home loan was serviced by AFR beginning approximately six years prior to the Data Breach. Plaintiff Zelenski and her husband were required to provide detailed personal and financial information to AFR in order to do business with the company. Such information included their names, Social Security numbers, and driver's license numbers. In maintaining Plaintiff Zelenski's information, Defendant expressly and impliedly promised to safeguard Plaintiff Zelenski's PII. Defendant, however, did not take proper care of Plaintiff Zelenski's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In March of 2022, Plaintiff Zelenski received a notification letter from Defendant stating that her PII, which included Plaintiff Zelenski's name, Social Security number, and driver's license number, was compromised.

10. The letter also offered one year of identity monitoring through Kroll, which was and continues to be ineffective for Plaintiff Zelenski and the Class members. In order to receive the free identity monitoring services, Plaintiff Zelenski would have had to share additional sensitive private information with third parties connected to AFR.

11. In the months and years following the Data Breach, Plaintiff Zelenski and Class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in customers' names, and targeted advertising without consent.

12. These harms are not just theoretical. Plaintiff Zelenski and her husband have already spent close to ten hours on the phone, monitoring their credit accounts, and attempting to learn more about the scope of the Data Breach from Defendant..

13. Plaintiff Zelenski and her husband greatly value their privacy, especially in the administration of their finances, and would not have done business with AFR if they had known that their information would be maintained using inadequate data security systems.

B. Defendant

14. Defendant American Financial Resources, Inc. is a full-service mortgage lender that operates nationally, including in Pennsylvania. AFR registered its headquarters at 9 Sylvan Way in Parsippany, New Jersey 07054. AFR's corporate policies and practices, including those used for data privacy, are established in, and emanate from the state of New Jersey.

JURISDICTION AND VENUE

15. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

16. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

17. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTS

18. Defendant services thousands of loans through mortgage brokers, bankers, lenders, homeowners, home buyers, realtors, and contractors across the country. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiff and the Class in accordance with all applicable law.

19. Defendant learned of an incident that occurred between December 6 and December 20, 2021, in which a "security incident" allowed an unauthorized actor to access AFR customers' Private Information including names, Social Security numbers, and driver's license numbers. Defendant sent the following notice letter template to various state attorneys general:[1]

> American Financial Resources ("AFR") understands the importance of protecting the information that we maintain. We are writing to inform you of an incident that involves some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.
>
> We recently concluded an investigation into a security incident involving some of our computer systems. Upon learning of the incident, we secured our network, launched an investigation, and notified law enforcement. Through the investigation, we determined that certain AFR files were accessed without authorization between December 6 – 20, 2021. AFR conducted a comprehensive review of the files that were accessed and, on February 4, 2022, determined that a file contained your . . .
>
> We wanted to notify you of the incident and assure you that we take it very seriously. We also encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institutions immediately.
>
> Additionally, AFR is offering you a complimentary one-year membership to Kroll's identity monitoring services. This service helps detect possible misuse of your personal information and

[1] Montana Attorney General's Office, *American Financial Resources, Inc. Data Notification Letter*, https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-264.pdf

> provides you with identity monitoring services focused on immediate identification and resolution of identity theft. This service is completely free to you and activating this program will not hurt your credit score. For more information about Kroll's identity monitoring, including instructions on how to activate your complimentary one-year membership, please visit https://enroll.krollmonitoring.com. You have until . . . to activate your identity monitoring services. Your membership number to activate is . . .
>
> We apologize for any inconvenience this incident may cause you. To help prevent something like this from happening in the future, we have implemented additional measures to enhance our existing security protocols. These measures include deploying a new advanced endpoint detection and response tool, resetting user passwords, upgrading server and domain controller software, and enhancing multifactor authentication. We also notified law enforcement and are cooperating with their investigation.

20. Upon learning of the Data Breach in December of 2021, Defendant investigated. Although Defendant has not provided an estimate of how many customers were affected by the Data Breach, Defendant reported that the incident affected customers in multiple states including California, Montana, Massachusetts, and Vermont.[2]

21. In March of 2022 Defendant announced through notice letters sent to customers and notifications to various state attorneys general that it had concluded an investigation into the data breach incident on February 4, 2022.

22. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected customers, which resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

[2] Various states require that data breach incidents affecting citizens within that state be reported to the attorney general's office within a reasonable period of time after the breach. Defendant sent notice of the Data Breach to several states and its generic notice letter is recorded in multiple state attorneys general consumer protection data breach portals. *See, e.g.*, *id.*

23. AFR's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many customers were affected by the Data Breach. Even worse, AFR offered only one year of identity monitoring for Plaintiff and Class members, which required their disclosure of additional PII with which AFR had just demonstrated it could not be trusted.

24. Plaintiff and Class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and Class members' unencrypted, unredacted information, including names, addresses, Social Security numbers, and driver's license numbers.

25. The Breach occurred because Defendant failed to take reasonable measures to protect the Private Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this release of information, despite repeated warnings to financial companies about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

26. Defendant disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class members was compromised through unauthorized

access. Plaintiff and Class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

27. AFR made, and continues to make, various promises to its customers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

28. In its Notice of Privacy Practices, which was updated for 2021, and therefore applicable to Plaintiff, Defendant stated under a section bolded and titled "Gathering, Using, and Sharing Information," the following:[3]

> You may interact with us in a variety of ways online, including through a mobile device. We may offer sites or applications that permit browsing and do not require registration. We may also offer the ability to enroll, register or access your accounts online. Information that we may collect about you through online interaction includes information that you input, such as your name, address, email address, other contact information; data resulting from your activity, such as transaction information; and location information. We may also gather additional information, such as the type of device and browser you are using, the IP address of your device, information about your device's operating system, and additional information associated with your device. We may also gather information collected through cookies, tags, and other technologies, as described further below.
>
> The types of personal information we collect and share depend on the product or service you have with us. This information may include:
>
> - Social Security number and employment information including tax returns, w-2s, paystubs and related documents
> - Account balances and transaction history
> - Credit history and investment experience
> - Social Security Number

[3] *Privacy Statement*, AM. FIN. RESOURCES (Feb. 1, 2021), https://www.afrcorp.com/privacy-statement/

- Current and previous home ownership experience, including physical and mailing addresses

- Letters of explanation regarding credit or employment events

- Date of birth / age

- Other information required by our investors or insurers (such as HUD)

Social Security numbers are classified as "Confidential" information under the AFR Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to AFR employees and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by AFR in connection with customer, employee, or other relationships.

29. AFR describes how it may use and disclose financial information for each category of uses or disclosures, none of which provide it a right to expose customers' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

30. By failing to protect Plaintiff's and Class members' Private Information, and by allowing the Data Breach to occur, AFR broke these promises to Plaintiff and Class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customer's Private Information

31. AFR acquires, collects, and stores a massive amount of its customers' protected PII, including financial information and other personally identifiable data.

32. As a condition of engaging in financial and mortgage-related services, AFR requires that these customers entrust them with highly confidential Private Information.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class members' Private Information, AFR assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class members' Private Information from disclosure.

34. Defendant had obligations created by industry standards, common law, and representations made to Plaintiff and Class members, to keep the Private Information confidential and to protect it from unauthorized access and disclosure.

35. Defendant failed to properly safeguard Class members' Private Information, allowing hackers to access their Private Information.

36. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

37. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

38. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

39. In fact, Defendant has been on notice for years that Plaintiff's and Class members' PII was a target for malicious actors. Despite such knowledge, AFR failed to implement and maintain reasonable and appropriate security measures to protect Plaintiff's and Class members' PII from unauthorized access AFR should have anticipated and guarded against.

40. Defendant was also on notice that the federal government has been concerned about data security. In 2021, the Federal Trade Commission "FTC" updated its consumer information Safeguards Rule, requiring non-banking financial institutions such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain comprehensive security systems to keep their customer's information safe. Against the backdrop of a rapid increase in cybersecurity incidents related to consumer financial information, Samuel Levine, the director of the FTC's Bureau of Consumer Protection The warning stated that "Financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it."[4]

41. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[6] That trend continues. The First American Financial Mortgage data breach incident in 2019, for example, exposed hundreds of millions of users' financial information to cybercriminals.[7]

42. The average time to identify and contain a data breach is 287 days,[8] with some breaches going unrecognized for months leading to costly recover efforts and financial impact. Additionally, the median cost per US consumer incurred on each fraud-related data breach incident

[4] *FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches*, https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-following-widespread-data

[5] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.

[6] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.

[7] *First American Financial Breach Exposes Millions of Complete Identities*, IDENTITY THEFT RESOURCE CTR (MAY 28, 2019), https://www.idtheftcenter.org/post/first-american-financial-breach-exposes-millions-of-complete-identities/.

[8] IBM SECURITY, COST OF A DATA BREACH REPORT 6 (2021) [hereinafter COST OF A DATA BREACH REPORT]

in 2020 was $450.[9] Data breaches and identity theft have a crippling effect on individuals and detrimental impact on the economy as a whole.[10]

43. A 2021 study conducted by Verizon showed that internal mismanagement of data security, including mis-delivery of emails, represents nearly 44 percent of the data breaches in the financial sector.[11] The majority of these incidents involve the sending or releasing of information to unauthorized actors.[12]

44. PII related data breaches continued to rapidly rise into 2021 when AFR was breached.[13]

45. Almost half of the data breaches globally are caused by internal errors, either human mismanagement of sensitive information, or system errors.[14] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[15] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[16]

46. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[17]

---

[9] Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime* (2020), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#top

[10] *Id.*

[11] *Financial and Insurance Data Breaches*, VERIZON 2021 DIBR DATA BREACH SURVEY (2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/.

[12] *Id.*

[13] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

[14] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.

[15] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

[16] *Id.*

[17] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

47. To prevent and detect unauthorized access, including the systems changes that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

48. To prevent and detect unauthorized access to its systems, including the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[18]

49. To prevent the unauthorized access that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information

[18] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

50. These are basic, common-sense email security measures that every business, not only those who handle sensitive financial information, should be doing. AFR, with its heightened standard of care should be doing even more. But by adequately taking these common-sense solutions, AFR could have prevented this Data Breach from occurring.

51. Charged with handling sensitive PII including financial information, AFR knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on AFR's customers as a result of a breach.

[19] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

AFR failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

52. With respect to training, AFR specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

53. The PII was also maintained on AFR's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's negligently maintained systems. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiff's and Class members' PII was a known risk to AFR, and thus AFR was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

54. The fact that Plaintiff's and Class members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

55. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiff and Class members is highly sensitive and of significant property value to those who would use it for wrongful purposes.

56. Private Information is a valuable property right that is an important commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an

array of crimes including identify theft and financial fraud.[20] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive financial information on multiple underground Internet websites, commonly referred to as the dark web.

57. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

58. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 billion per year online advertising industry in the United States.[22]

59. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[23]

---

[20] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

21 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

[22] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[23] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

60. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[24] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

61. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[25]

62. The value of Plaintiff's and Class members' Private Information on the black market is substantial. Sensitive financial information can sell for as much as $1000.[26] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's information.

63. The ramifications of AFR's failure to keep its customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

---

24 *Web's Hot New Commodity*, *supra* note 17.

25 *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

26 *See* Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Nov. 21, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/

64. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[27] This gives thieves ample time to make fraudulent charges under the victim's name.

65. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the financial industry and related industries.

66. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the ransomware attack into its systems and, ultimately, the theft of its customers' Private Information.

67. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[28] For example, different PII elements from various sources may be able to be linked in order to

[27] *See Medical ID Theft Checklist*, IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[28] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

identify an individual, or access additional information about or relating to the individual.[29] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and Class members that was misused.

68. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

69. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

70. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

71. Acknowledging the damage to Plaintiff and Class members, Defendant instructed customers like Plaintiff to "review[] your account statements and credit reports for any unauthorized activity." Plaintiff and the other Class members now face a greater risk of identity theft.

[29] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

72. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names. Plaintiff and Class members have a property interest in their information and were deprived of this property when it was released to unauthorized actors through the negligent maintenance of Defendant's systems.

D. AFR Failed to Comply with FTC Guidelines

73. AFR was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. §45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

74. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[30]

75. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[31] The guidelines note that businesses should protect the personal customer information that they keep; 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 any security problems.

---

[30] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].

[31] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.

76. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private 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.[32]

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

78. AFR was at all times fully aware of its obligation to protect the Private Information of customers because of its position as a trusted mortgage lender. AFR was also aware of the significant repercussions that would result from its failure to do so.

E. Damages to Plaintiff and the Class

79. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

80. The ramifications of AFR's failure to keep customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information

[32] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter Start with Security].

and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[33]

81. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

82. Defendant further owed and breached its duty to Plaintiff and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

83. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and Class members' Private Information as detailed above, and Plaintiff and Class members are now at a heightened and increased risk of identity theft and fraud.

84. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of

[33] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

85. Some of the risks associated with the loss of personal information have already manifested themselves in Plaintiff Zelenski's case. Plaintiff Zelenski received a cryptically written notice letter from Defendant stating that her information was released, and that she should remain vigilant of fraudulent activity on her accounts, with no other explanation of where this information could have gone, or who might have access to it. Plaintiff Zelenski has already spent hours on the phone trying to determine what negative effects may occur from the loss of her personal information.

86. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, and similar identity theft.

87. Plaintiff and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

88. Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with AFR. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

89. Plaintiff and Class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

90. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

91. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[34] The SSA has stated that "[i]dentity 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."[35] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[36]

92. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[37]

93. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. Private Information can be used to submit false insurance claims. As a result, Plaintiff and Class members now face a real and continuing immediate risk of identity theft and other

34 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.
35 *Id.*
36 *Id.*
37 *Id.*

problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. For Plaintiff and Class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

94. As a result of the Data Breach, Plaintiff and Class members' Private Information has diminished in value.

95. The Private Information belonging to Plaintiff and Class members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiff and the class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

96. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and Class members' Private Information 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' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

97. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

98. Defendant did not properly train their employees to identify and avoid unauthorized access to the network.

99. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff's and Class members' Private Information.

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

101. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent 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."[38]

102. Other than offering one year of identity monitoring, Defendant did not take any measures to assist Plaintiff and Class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;

[38] *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff's and Class members' Private Information.

103. Defendant's failure to adequately protect Plaintiff's and Class members' Private Information has resulted in Plaintiff and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as AFR's Data Breach Notice indicates, it is putting the burden on Plaintiff and Class members to discover possible fraudulent activity and identity theft.

104. While Defendant offered one year of identity monitoring, Plaintiff could not trust a company that had already breached her data. The identity monitoring offered from Kroll does not guarantee privacy or data security for Plaintiff, who would have to expose her information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and Class members are now burdened with indefinite monitoring and vigilance of their accounts.

105. Moreover, the offer of one year of identity monitoring to Plaintiff and Class members is woefully inadequate. While some harm has already begun, 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 Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent

identity theft.[39] This is especially true for many kinds of financial identity theft, for which most identity monitoring plans provide little or no monitoring or protection.

106. Plaintiff and Class members have been damaged in several other ways as well. Plaintiff and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and Class members also suffered a loss of the inherent value of their Private Information.

107. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Plaintiff and Class members to defraud them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

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

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

[39] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

- 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;

- The continued risk to their Private Information, 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 Private Information in its possession;

- 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; and

- Anxiety and distress resulting fear of misuse of their Private Information.

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

CLASS ACTION ALLEGATIONS

110. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23.

111. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Nationwide Class and Pennsylvania Subclass (collectively defined herein as the "Class"):

Nationwide Class

> All persons nationwide whose Private Information was compromised as a result of the Data Breach discovered on or about December 2021 and who were sent notice of the Data Breach.

Pennsylvania Subclass

> All persons residing in Pennsylvania whose Private Information was compromised as a result of the Data Breach discovered on or about December of 2021 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

112. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

113. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class numbers in the thousands.

114. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private

Information from unauthorized capture, dissemination, and misuse;

- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

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

116. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

117. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because her interests do not conflict with the interests of the Classes she seeks to represent, she has retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

118. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

119. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** 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 class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases 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 a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

120. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

121. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

122. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

123. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

124. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to

unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

125. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

126. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class members' Private Information.

127. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and Class members' Private Information.

128. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiff and Class members, Defendant had a duty to adequately protect its data systems and the Private Information contained thereon.

129. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

130. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted, and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

131. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant are bound by industry standards to protect confidential Private Information.

132. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

133. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to detect in a timely manner that Class members' Private Information had been compromised; and

  Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

134. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff's and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession or control.

135. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

136. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

137. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

138. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free identity monitoring to all Class members.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

139. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

140. Plaintiff and Class members entered into valid and enforceable express contracts with Defendant under which Plaintiff and other Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide financial services and, impliedly, if not explicitly, agreed to protect Plaintiff's and Class members' Private Information.

141. To the extent Defendant's obligation to protect Plaintiff's and other Class members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and other Class members' Private Information, including in accordance with trade regulations; federal, state and local laws; and industry standards. No Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiff's and other Class members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

142. A meeting of the minds occurred, as Plaintiff and other Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

143. The protection of Plaintiff and Class members' Private Information were material aspects of Plaintiff's and Class members' contracts with Defendant.

144. Defendant's promises and representations described above relating to industry practices, and about Defendant's purported concern about its clients' privacy rights became terms of the contracts between Defendant and its clients, including Plaintiff and other Class members. Defendant breached these promises by failing to comply with reasonable industry practices.

145. Plaintiff and Class members read, reviewed, and/or relied on statements made by or provided by AFR and/or otherwise understood that AFR would protect its customers' Private Information if that information were provided to AFR.

146. Plaintiff and Class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

147. As a result of Defendant's breach of these terms, Plaintiff and other Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiff and Class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

148. Plaintiff and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

149. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

150. Plaintiff brings this claim for breach of implied contract alternatively to her breach of contract claim.

151. Through their course of conduct, Defendant, Plaintiff, and Class members entered into implied contracts for the provision of financial services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information.

152. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when she first entered into the financial services agreement with Defendant.

153. The valid and enforceable implied contracts to provide financial services that Plaintiff and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

154. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

155. Defendant solicited and invited Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offers and provided their Private Information to Defendant.

156. In entering into such implied contracts, Plaintiff and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

157. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

158. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide financial services to Plaintiff and Class members; and (b) protect Plaintiff's and the Class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

159. Both the provision of financial services and the protection of Plaintiff's and Class members' Private Information were material aspects of these implied contracts.

160. The implied contracts for the provision of financial services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

161. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff's and Class members Private Information.

162. Consumers of financial services value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to

Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

163. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant and/or its affiliated companies, and paid for the provided services in exchange for, amongst other things, both the provision of financial services and the protection of their Private Information.

164. Plaintiff and Class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

165. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

166. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and Class members' Private Information as evidenced by its notifications of the Data Breach to Plaintiff and Class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class members' private information as set forth above.

167. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

168. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive full benefit of the bargain, and instead received financial and other services that were of a diminished value to that described in the contracts. Plaintiff and Class members therefore were damaged in an amount at least equal to

the difference in the value of the lending services with data security protection they paid for and the services they received.

169. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, Class members, nor any reasonable person would have utilized services from Defendant and/or its affiliated entities.

170. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

171. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

172. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate identity monitoring to all Class members.

COUNT IV
Unjust Enrichment/Quasi-Contract
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

173. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

174. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with

their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

175. Defendant knew that Plaintiff and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from Plaintiff's and Class members' purchases and used Plaintiff's and Class member's Private Information for business purposes.

176. Defendant failed to secure Plaintiff and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff and Class members' Private Information provided.

177. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

178. If Plaintiff and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have used Defendant's services.

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

180. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred on them.

181. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and the Class members overpaid for the use of Defendant's services.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

182. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

183. In providing their Private Information to Defendant, Plaintiff and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and Class members to safeguard and keep confidential that Private Information.

184. Defendant accepted the special confidence Plaintiff and Class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiff's] personal information" as included in the Data Breach notification letter.

185. In light of the special relationship between Defendant and Plaintiff and Class members, whereby Defendant became a guardian of Plaintiff's and Class members Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class members for the safeguarding of Plaintiff and Class member's Private Information.

186. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of its customer's relationship, in particular, to keep secure the Private Information of its customers.

187. Defendant breached its fiduciary duties to Plaintiff and Class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's Private Information.

188. Defendant breached its fiduciary duties to Plaintiff and Class members by otherwise failing to safeguard Plaintiff's and Class members' Private Information.

189. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

190. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Breach of Confidence
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

191. Plaintiff incorporates by reference paragraphs 1-12, as though fully set forth herein.

192. At all times during Plaintiff and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiff's and the Class members' Private Information that Plaintiff and Class members provided to Defendant.

193. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by expectations that Plaintiff and Class members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

194. Plaintiff and Class members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

195. Plaintiff and Class members also provided their respective Private Information to Defendant with the explicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

196. Defendant voluntarily received in confidence Plaintiff and Class members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

197. Due to Defendant's failure to prevent, detect, and/or avoid the Security Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's and Class members' Private Information, Plaintiff's and Class members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class members' confidence, and without their express permission.

198. But for Defendant's disclosure of Plaintiff's and Class members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Security Breach was the direct and legal cause of the theft of Plaintiff's and Class members' Private Information, as well as the resulting damages.

199. The injury and harm Plaintiff and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class members' Private Information. Defendant knew or should have known its security systems were insufficient to protect the Private Information that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

200. As a direct and proximate cause of Defendant's conduct, Plaintiff and Class members suffered damages as alleged above.

COUNT VII
Bailment
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

201. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

202. Plaintiff and Class members delivered and entrusted their Personal Information to Defendant for the sole purpose of receiving services from Defendant.

203. In delivering their Personal Information to Defendant, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their personal and financial information.

204. Defendant accepted possession of Plaintiff's and Class members' Personal Information. By accepting possession, Defendant understood that Plaintiff and Class members expected Defendant to safeguard their personal and financial information adequately. Accordingly, a bailment was established for the mutual benefit of the parties.

205. During the bailment, Defendant owed a duty to Plaintiff and Class members to exercise reasonable care, diligence, and prudence in protecting their Personal Information.

206. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' Personal Information, resulting in the unlawful and unauthorized access to and misuse of such information.

207. Defendant further breached its duty to safeguard Plaintiff's and Class members' Personal Information by failing to notify them individually in a timely and accurate manner that their information had been breached and compromised.

208. As a direct and proximate result of Defendant's breach of duty, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

COUNT VIII
Violations of the New Jersey Consumer Fraud Act
(N.J. Stat. Ann. § 56:8-2, *et seq.*)
(On Behalf of Plaintiff and the Nationwide Class)

209. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

210. The New Jersey Consumer Fraud Act (New Jersey CFA) makes unlawful "[t]he act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing concealment, suppression

or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby." N.J. Stat. Ann. § 56:8-2.

211. By the acts and conduct alleged herein, Defendant committed unfair or deceptive acts and practices by:

a. failing to maintain adequate computer systems and data security practices to safeguard Plaintiff and the Class's PII;

b. failing to disclose that its computer systems and data security practices were inadequate to safeguard PII from theft;

c. continuing to gather and store PII and other personal information after Defendant knew or should have known of the security vulnerabilities of its computer systems that were exploited in the Data Breach; and,

d. continuing to gather and store PII and other personal information after Defendant knew or should have known of the unauthorized access and before Defendant allegedly remediated the data security incident.

212. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, the Gramm- Leach-Bliley Act, and the New Jersey CFA.

213. The foregoing deceptive acts and practices were directed at New Jersey consumers/purchasers.

214. Defendant, Plaintiff, and Class members are "persons" within the meaning of N.J. Stat. Ann. § 56:8-2(d).

215. Defendant engaged in "sales" of "merchandise" within the meaning of N.J. Stat. Ann. § 56:8-2(c) & (d).

216. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the financial services provided, specifically as to the safety and security of Plaintiff and the Class's Private Information, and induce consumers to purchase the same.

217. Defendant's unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in the above paragraphs are material in that they relate to matters which reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their purchasing decisions or conducting themselves regarding the purchase of services from Defendant.

218. Class members are New Jersey consumers who made payments to Defendant for the furnishing of financial services that were primarily for personal, family, or household purposes.

219. Defendant engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of services to consumers, including Plaintiff and Class members. Defendant's acts, practices, and omissions were done in the course of Defendant's business of marketing, offering to sell, and furnishing of loan services to consumers in the State of New Jersey. As a direct and proximate result of Defendant's multiple, separate violations of N.J. Stat. Ann. § 56:8-2, Plaintiff and the Class members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and

future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class members; and (vii) the diminished value of Defendant's services they received.

220. Also, as a direct result of Defendant's violation of the New Jersey Consumer Fraud Act, Plaintiff and the Class members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate identity monitoring to all Class members. Plaintiff and Class members were injured because: a) they would not have purchased services from Defendant had they known the true nature and character of Defendant's data security practices; b) Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of promises that Defendant would keep their information reasonably secure, and c) Plaintiff and Class members would not have entrusted their PII to Defendant in the absence of the promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

221. As a result, Plaintiff and the Class members have been damaged in an amount to be proven at trial.

222. On behalf of themselves and other members of the Class, Plaintiff is entitled to recover legal and/or equitable relief, including an order enjoining Defendant's unlawful

conduct, treble damages, costs, and reasonable attorneys' fees pursuant to N.J. Stat. Ann. § 56:8-19, and any other just and appropriate relief.

COUNT IX
Violations of the Pennsylvania Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. §§ 201-1 to 201-9.2 ("UTPCPL"))
(On Behalf of Plaintiff and the Pennsylvania Subclass)

223. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

224. Plaintiff and Defendant are each a "person" as defined in 73 Pa. Stat. § 201-2(2).

225. Plaintiff and the Pennsylvania Subclass members purchased goods and services in "trade" and "commerce" as defined by73 Pa. Stat. §§ 201-2(3).

226. Plaintiff and the Pennsylvania Subclass purchased goods and services primarily for personal, family, and/or household purposes under 73 Pa. Stat. § 201-9.2.

227. Defendant engaged in "unfair methods of competition" or "unfair or deceptive acts or practices" as defined in 73 Pa. Stat. § 201-2(4) by engaging in the following conduct:

a. Representing that its goods and services had characteristics, uses, benefits, and qualities that they did not have—namely that its goods, services, and business practices were accompanied by adequate data security (73 Pa. Stat. § 201-2(4)(v));

b. Representing that its goods and services were of a particular standard or quality when they were of another quality (73 Pa. Stat. § 201-2(4)(vii));

c. Representing that its goods and services were of a particular standard or quality when they were of another quality (73 Pa. Stat. § 201-2(4)(ix); and

d. "engaging in any other . . . deceptive conduct which creates a likelihood of confusion or misunderstanding" (73 Pa. Stat. § 201-2(4)(xxi)).

228. These unfair methods of competition and unfair or deceptive acts or practices are declared unlawful by 73 Pa. Stat. § 201-3.

229. Defendant's unfair or deceptive acts and practices include but are not limited to: failing to implement and maintain reasonable data security measures to protect Plaintiff and the Pennsylvania Subclass members' information; failing to identify foreseeable data security risks and remediate the identified risks; failing to comply with common law duties, industry standards including PCI DSS, and FTC guidance regarding data security; misrepresenting in its Privacy Policy that it would protect

Plaintiff and the Pennsylvania Subclass member's Private Information; and omitting and concealing the material fact that it did not have reasonable measures in place to safeguard their Private Information.

230. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security practices and ability to protect their Private Information.

231. Defendant intended to mislead consumers and induce them to rely on its misrepresentations and omissions. As set forth herein, Plaintiff and the Pennsylvania Subclass members did rely on Defendant's misrepresentations and omissions relating to its data privacy and security.

232. Plaintiff and Pennsylvania Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered with reasonable diligence.

233. Had Defendant disclosed to Plaintiff and Pennsylvania Sublcass members that its data security systems were not secure and, thus, were vulnerable to attack, Plaintiff and Pennsylvania Subclass members would not have given their financial information to Defendant.

234. Defendant acted intentionally, knowingly, and maliciously in violating the Pennsylvania UTPCPL, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights.

235. Data breaches put Defendant on notice of the importance of data security and that its systems are subject to attack.

236. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and the Pennsylvania Subclass have suffered and will continue to suffer damages, injury, ascertainable losses of money or property, and monetary and non-monetary damages as described above.

237. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including the following as expressly permitted under 73 Pa. Stat. § 201-9.2:

a. "actual damages or [statutory damages of] one hundred dollars ($100), whichever is greater";

b. treble damages, defied as "three times the actual damages";

c. "reasonable attorney fees" and litigation costs; and

d. "such additional relief as [the Court] deems necessary or proper."

238. Plaintiff and Pennsylvania Subclass members also seek the injunctive relief as set forth above and throughout this Complaint.

COUNT X
Declaratory Relief
(On Behalf of Plaintiff and the Nationwide Class, or Alternatively, Plaintiff and the Pennsylvania Subclass)

239. Plaintiff incorporates by reference paragraphs 1-119, as though fully set forth herein.

240. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

241. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' PII, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their PII will occur in the future.

242. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

243. Defendant still possesses the PII of Plaintiff and the Class.

244. To Plaintiff's knowledge, Defendant has made no changes to its data storage or security practices relating to the PII.

245. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

246. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at AFR. The risk of another such breach is real, immediate, and substantial.

247. The hardship to Plaintiff and Class members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at AFR, Plaintiff and Class members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

248. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AFR, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose PII would be further compromised.

249. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant implement and maintain reasonable security measures, including but not limited to the following:

- Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on AFR's systems on a periodic basis, and ordering AFR to

promptly correct any problems or issues detected by such third-party security auditors;

- engaging third-party security auditors and internal personnel to run automated security monitoring;
- auditing, testing, and training its security personnel regarding any new or modified procedures;
- purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;
- conducting regular database scans and security checks; and
- routinely and continually conducting 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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained by Defendant as a result of its wrongful conduct;

E. Ordering Defendant to pay for no less than three (3) years of identity monitoring services for Plaintiff and the Class;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Date: April 26, 2021

Respectfully submitted,

/s/ Gary S. Graifman, Esq._____
Gary S. Graifman
Melissa R. Emert*
KANTROWITZ, GOLDHAMER & GRAIFMAN, P.C.

135 Chestnut Ridge Road, Suite 200
Montvale, New Jersey 07645
T: 845-356-2570
F: 845-356-4335
ggraifman@kgglaw.com
memert@kgglaw.com

*pro hac vice to be filed

Attorneys for the Plaintiff and the Putative Classes