Elaine A. Ryan (AZ Bar #012870)
Colleen M. Auer (AZ Bar #014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
520-705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

Jean S. Martin
(Pro Hac Vice application forthcoming)
Ra O. Amen
(Pro Hac Vice application forthcoming)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
JeanMartin@ForThePeople.com
RAmen@ForThePeople.com

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ARIZONA

Joshua Quinalty, on behalf of himself and all others similarly situated, Plaintiff, v. FocusIT, LLC, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Joshua Quinalty ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated against Defendant FocusIT, LLC ("FocusIT" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

NATURE OF THE ACTION

1. On August 2, 2022, FocusIT, LLC—a third-party vendor hosting mortgage origination and loan processing software applications for banks and financial institutions—was notified by the Texas Financial Crimes Intelligence Center that unknown cybercriminals compromised a system in the FocusIT environment (the "Data Breach" or "Breach").[1]

2. This Breach resulted in Plaintiff's and Class Members' personal identifying information ("PII"), including the names, dates of birth, addresses, and Social Security numbers of 147,799 individuals being accessed by cybercriminals.[2] Upon information and belief, Defendant obtained Plaintiff's and Class Members' PII from the banks and financial institutions that Defendant services. Customer PII associated with 32 banks and financial institutions that Defendant services was compromised in the Breach.[3] Upon information and belief, Plaintiff and Class Members are former and present customers, applicants, and account holders of the banks and financial institutions that Defendant services.

3. As a result of FocusIT's failure to properly secure its network and implement proper intrusion detection tools, unknown cybercriminals gained unfettered access to Plaintiff's and Class Members' PII from June 1, 2022 to August 3, 2022, *i.e.*, *for over two months*.

4. Not only did FocusIT fail to properly protect Plaintiff's and Class Members' PII, it also failed to timely notify Plaintiff and Class Members of the Data Breach, waiting more than three months to send letters to impacted persons.

5. When Defendant finally announced the Data Breach, it underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's Breach notice letter

[1] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf (last visited December 26, 2022) at 1.

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/f7a54169-98e6-47b4-9f66-fb33ebe0c1ee.shtml.

[3] https://oag.ca.gov/ecrime/databreach/reports/sb24-557773.

(the "Notice")[4] sent to affected individuals failed to explain how many people were impacted, how the breach happened, or why it took over three months to send a bare-bones notice to impacted persons.

6. Upon information and belief, cybercriminals were able to breach Defendant's systems because it did not maintain reasonable security safeguards or protocols to protect its Plaintiff's and Class Members' PII, leaving it an unguarded target for theft and misuse.

7. Defendant's failure to timely detect and notify breach victims violated Arizona law and made Plaintiff and Class Members vulnerable to identity theft without a timely warning to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant is offering free credit monitoring services for only a year.[5] This is insufficient protection for those impacted by the Data Breach as their PII was taken by unknown cybercriminals and can be used at any time in the future. Further, Defendant's offering will not prevent the unauthorized use of impacted persons' PII and will merely serve to (possibly and hopefully) notify them if and when their PII is used.

9. Defendant knew or should have known that each victim of the Data Breach deserved prompt and sufficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

10. Defendant's misconduct has caused damages to the Plaintiff and members of the proposed Class, including: (i) the lost or diminished value of their PII; (ii) costs associated with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive PII.

---

[4] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf.

[5] *Id.*

11. Plaintiff and members of the proposed Class therefore bring this lawsuit seeking damages and relief for Defendant's actions.

PARTIES

12. Plaintiff Joshua Quinalty is a natural person and citizen of Oklahoma, residing in Tuttle, Oklahoma.

13. Defendant FocusIT, LLC is an Arizona limited liability company with its headquarters and principal place of business at 14362 N. Frank Lloyd Wright Blvd., Suite 1000, Scottsdale, Arizona 85260 in Maricopa County. FocusIT, LLC was formerly FocusIT, Inc., an Arizona corporation, but converted to a limited liability company on January 1, 2023.

JURISDICTION AND VENUE

14. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

15. This Court has personal jurisdiction over Defendant because Defendant is headquartered in Arizona and conducts substantial business in this District.

16. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District, and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendant's Failure to Safeguard Patients' PII

17. Defendant is a third-party vendor of financial and information technology services and products, including mortgage origination and loan processing software

applications for banks and financial institutions.[6] Defendant also offers hosting of said mortgage origination and loan processing software applications for banks and financial institutions.

18. Plaintiff and Class Members' PII was provided to Defendant in conjunction with the type of work Defendant does within the financial industry, and specifically the financial software industry.

19. Upon information and belief, Defendant maintains the PII of customers of its business partners, such as full names, Social Security Numbers, financial account information and/or credit-card information, dates of birth, and addresses. These records are stored on Defendant's computer network.

20. Upon information and belief, Defendant received Plaintiff and Class Members' PII from its various customers and business partners in the financial industry, specifically the financial software industry.

21. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, Defendant knew or reasonably should have known that it must comply with industry standards related to data security and all federal and state laws protecting customer PII and provide adequate notice to customers if their PII is disclosed without proper authorization.

22. Defendant represents in its Privacy Policy that, "We follow generally accepted industry standards to protect Personal Information…."[7]

23. Upon information and belief, prior to collecting this sensitive information, Defendant misrepresented—(1) to the public, including its customers, Plaintiff, and Class Members and (2) via its contracts, website, Privacy Policy, and general advertising and sales communications—that it uses reasonable measures to safeguard from theft and

[6] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf (last visited December 26, 2022) at 1.

[7] https://www.focusitinc.com/privacy-statement/ (last visited January 27, 2023).

misuse the PII it obtains from its customers. These misrepresentations were designed to mislead the public and were, in fact, passed on from Defendant's customers to consumers, including Plaintiff and Class Members.

24. Upon information and belief, Defendant omitted to disclose to the public, including its customers, Plaintiff, and Class Members via its contracts, website, Privacy Policy, and other advertising and sales communications its failure to use reasonable measures to safeguard from theft and misuse the PII it obtains from its customers. These omissions were designed to mislead the public and were, in fact, passed on from Defendant's customers to consumers, including Plaintiff and Class Members.

25. Upon information and belief, Defendant acquired, collected, and stored, and represented that it maintained reasonable security over Plaintiff's and Class Members' PII.

26. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew, or should have known, that it was thereafter responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

27. Upon information and belief, Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

28. Had Plaintiff and members of the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

29. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

30. Defendant could have prevented the Data Breach by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII.

31. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

32. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII from being compromised:

a. Upon information and belief, Defendant was unable to determine the extent to which Plaintiff's and Class Members' PII was accessed or compromised. Accordingly, Defendant failed to properly monitor and log the ingress and egress of network traffic, file access, and file modifications.[8]

b. Defendant failed to properly train its employees as to cybersecurity best practices and to maintain proper staffing and processes for responding to and preventing network intrusions.[9]

c. Upon information and belief, Defendant failed to implement sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.[10]

---

[8] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf (stating that "unknown threat actor(s) *potentially* compromised a third party system in the FocusIT environment" and "your personal information [was] *potentially* being accessed by unknown threat actors").

[9] https://apps.web.maine.gov/online/aeviewer/ME/40/f7a54169-98e6-47b4-9f66-fb33ebe0c1ee.shtml (stating that the Breach resulted from a "phishing" attack).

[10] *Id.* (the Breach began on June 1, 2022 but was not discovered until August 2, 2022—over two months later—and not by Defendant but an unrelated, third party).

d. Upon information and belief, Defendant failed to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity to identify possible threats.[11]

e. Defendant failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class Members.

f. Defendant failed to timely and accurately disclose that Plaintiff's and Class Members' PII had been improperly acquired or accessed.

g. Defendant knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII.

h. Defendant failed to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiff and Class Members, misuse the PII and potentially disclose it to others without consent.

33. Prior to the Breach, Defendant was aware of its security failures but failed to correct them or to disclose them to the public, including Plaintiff and Class Members.

34. The implementation of proper encryption, logging, detection, training, and monitoring protocols requires affirmative acts. Accordingly, Defendant knew or should have known that it did not take such actions and failed to implement adequate data security practices.

35. As a result of Defendant's acts and omissions, Plaintiff and Class Members had their most sensitive Private Information stolen by malicious cybercriminals. The

[11] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf (stating that "your personal information [was] *potentially* being accessed by unknown threat actors").

information that was compromised is a one-stop shop for identity thieves to wreak havoc on Plaintiff's and Class Members' personal and financial lives. Given the sensitivity and static nature of the information involved (such as Social Security numbers), the risk of identity theft is present, materialized, and will continue into the foreseeable future for Plaintiff and Class Members.

B. The Data Breach

36. On August 2, 2022, Defendant was notified by the Texas Financial Crimes Intelligence Center that unknown threat actor(s) compromised a system in the FocusIT environment.[12]

37. The Breach resulted in Plaintiff's and Class Members' PII, including the names, dates of birth, addresses and Social Security numbers of 147,799 individuals being accessed by cybercriminals.[13]

38. Although the Breach was discovered on August 2, 2022, the Breach actually began on June 1, 2022 and was not resolved until August 3, 2022. In other words, cybercriminals had unfettered access to Defendant's network for over two months. Such access only ended when the Breach was discovered, not by Defendant, but by an unrelated, third party.[14]

39. While Defendant's Notice fails to state the mechanism by which the Breach occurred, governmental authorities report that the Breach resulted from a "phishing" attack.[15]

---

[12] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf (last visited December 26, 2022) at 1.

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/f7a54169-98e6-47b4-9f66-fb33ebe0c1ee.shtml.

[14] https://apps.web.maine.gov/online/aeviewer/ME/40/f7a54169-98e6-47b4-9f66-fb33ebe0c1ee.shtml.

[15] https://oag.ca.gov/ecrime/databreach/reports/sb24-557773.

40. While Defendant's Notice fails to provide sufficient details on the Breach, one of Defendant's customers states:

> FocusIT contracted Arete, a cybersecurity forensics firm, to perform a comprehensive investigation and review of the reported breach occurrence. Arete completed their cyber forensics investigative review of FocusIT computer systems & applications on August 21, 2022. Their review indicated on Monday, July 25, 2022, a threat actor(s) posted & displayed login credentials of a FocusIT employee, possibly compromised through a phishing email, on the dark web for $ 300 in payment. The Texas Financial Crimes Intelligence Center and FocusIT contacted a "Russian speaking, threat actor" and negotiated payment to receive the database records. Josh Bopp, President and Arete, could not determine if others purchased the database records from the displayed FocusIT login credentials.[16]

41. Upon information and belief, Plaintiff's and Class Members' PII was accessed, exfiltrated, and/or stolen during the Breach.

42. Upon information and belief, Plaintiff's and Class Members' affected PII was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

43. It is likely the Data Breach was enacted by cybercriminals due to Defendant's status as a financial software company within the financial industry.

44. While Defendant claims to have become aware of the breach as early as August 2, 2022, Defendant did not begin notifying victims of the Data Breach until September 28, 2022, *nearly two months later*.[17]

45. Time is of the essence when highly sensitive PII is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiff and Class Members are now

---

[16] https://www.fmb1919.bank/FocusIT-Data-Breach.

[17] https://apps.web.maine.gov/online/aeviewer/ME/40/f7a54169-98e6-47b4-9f66-fb33ebe0c1ee.shtml.

subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII, especially their Social Security numbers, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers.

46. Following the Breach and recognizing that each Class Member is now subject to the present and continuing risk of identity theft and fraud, Defendant encouraged Plaintiff and Class Members to take several precautions. Defendant advised Plaintiff and Class Members that:

a. "You should monitor your financial accounts for any suspicious activity";

b. "The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically";

c. "You may also choose to place a fraud alert on your credit file"; and

d. If "you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the FTC."[18]

47. Defendant largely put the burden on Plaintiff and Class Members to take measures to protect themselves.

48. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.

49. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week; leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'" Usually, this time can be spent at the option and choice

[18] https://oag.ca.gov/system/files/FocusIT%20-%20General-Redacted.pdf.

of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

50. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and, thus, seek renumeration for the loss of valuable time as another element of damages.

51. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

52. Defendant also offered credit monitoring services for a period of 12 months. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

53. Defendant's Notice letter, as well as its website notice, both omit the size and scope of the breach. Defendant has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

54. Plaintiff and the Class Members remain, even today, in the dark regarding what particular data was stolen, the phishing attack used, and what steps are being taken, if any, to secure their PII going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

55. Plaintiff's and Class Members' PII may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and/or Class Members. Either way, unauthorized individuals can now easily access the PII of Plaintiff and Class Members.

C. Plaintiff's Experience

56. Upon information and belief, Plaintiff Quinalty is a current or former account holder or applicant associated with one of Defendant's customers.

57. Shortly after and as a result of the Data Breach, Plaintiff Quinalty was a victim of identity theft. Specifically, On June 20, 2022, Verizon notified him that two iPhones were purchased under his Verizon account. Plaintiff took steps to mitigate those fraudulent purchases. However, On October 31, 2022, Verizon informed him that two more iPhones were purchased under his account. Verizon informed him that an unauthorized user had gained access to his Verizon account using a fake ID that contained his personal information. As a result of this fraud, Plaintiff Quinalty suffered financial damages and was required to use his free time to mitigate the effects of the identity theft. Further, he was unable to obtain a new phone for a month because of these fraudulent purchases.

58. Shortly after and as a result of the Data Breach, Plaintiff Quinalty experienced an increase in spam and suspicious phone calls, texts, emails, and targeted advertisements.

59. On or about the first week of October 2022, more than two months after Defendant learned of the Data Breach and more than four months after the Breach began, Plaintiff Quinalty received a Notice letter from Defendant, notifying him that his PII had been exposed to unauthorized third parties and cyber criminals in the Breach.

60. As a result of the Data Breach, Plaintiff Quinalty purchased credit monitoring services, the cost of which were reasonable and necessary.

61. As a result of the Data Breach and Defendant's Notice letter and recommendations, Plaintiff Quinalty made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing his accounts for fraud.

62. Plaintiff Quinalty has spent approximately 12 hours responding to the Data Breach and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

63. Plaintiff Quinalty suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII.

64. Plaintiff Quinalty is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII, in combination with his name and Social Security number, being placed in the hands of unauthorized third parties/criminals. This injury was worsened by Defendant's two-month long delay in informing Plaintiff and Class Members about the Data Breach.

65. Plaintiff Quinalty has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

66. Plaintiff Quinalty had never been the victim of a data breach prior to Defendant's Data Breach.

D. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

67. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

68. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

69. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[19]

70. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

e. Lost opportunity costs and lost wages associated with the time and effort expended 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;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

[19] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited June 21, 2022).

71. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[20]

72. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

73. It can take victims years to spot identity or PII theft, giving criminals plenty of time to milk that information for cash.

74. One such example of criminals using PII for profit is the development of "Fullz" packages.[21]

75. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

---

[20] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 21, 2022).

[21] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/, (last visited June 21, 2022).

76. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

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

78. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII had been stolen.

79. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

80. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

81. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

82. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "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."[22]

83. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[23] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[24]

84. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[25] The FTC treats the failure to employ reasonable and

[22] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited June 21, 2022).

[23] *Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 21, 2022).

[24] *Id.*

[25] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012),

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

85. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII.

---

https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen (last visited June 21, 2022).

86. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[26] The next year, that number increased by nearly 45%.[27]

87. Charged with handling highly sensitive Personal Information including financial information, Defendant knew or should have known the importance of safeguarding the Personal Information that was entrusted to it. Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

88. Defendant disclosed the PII of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

89. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous operators, con artists and outright criminals.

90. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's

---

[26] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://bit.ly/30Gew91 [hereinafter "*Data Breaches Increase 40 Percent in 2016*"] (last visited June 21, 2022).

[27] *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, ITRC (Jan. 22, 2018), https://bit.ly/3jdGcYR [hereinafter "*Data Breaches Up Nearly 45 Percent*"] (last visited June 21, 2022).

injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendant Failed to Adhere to FTC Guidelines

91. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[28] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Personal Information.

92. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[29] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

93. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

94. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious

---

[28] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last visited June 21, 2022).

[29] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last visited June 21, 2022).

activity on the network; and verify that third-party service providers have implemented reasonable security measures.[30]

95. 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.

96. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this action on behalf of himself, and all members of the proposed Class (the "Class") pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) as defined as:

> All individuals residing in the United States whose PII was compromised in the Data Breach announced by Defendant on September 28, 2022.

98. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's

[30] *See Start with Security*, *supra* FN22.

counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

99. The Class defined above is identifiable through Defendant's business records.

100. Plaintiff reserves the right to amend the class definition.

101. This action is properly maintainable as a class action under Fed. R. Civ. P. 23.

102. **Numerosity.** Plaintiff is representative of the proposed Class, consisting of thousands of members, far too many to join in a single action.

103. **Commonality.** There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and members of the Class's PII;

b. Whether Defendant breached the duty to use reasonable care to safeguard members of the Class's PII;

c. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PII;

d. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and members of the Class's PII from unauthorized release and disclosure;

e. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff's and members of the Class's PII from unauthorized release and disclosure;

f. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

g. Whether Defendant's delay in informing Plaintiff and members of the Class of the Data Breach was unreasonable;

h. Whether Defendant's method of informing Plaintiff and other members of the Class of the Data Breach was unreasonable;

i. Whether Defendant's conduct was likely to deceive the public;

j. Whether Defendant is liable for negligence or gross negligence;

k. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII violated applicable state laws;

l. Whether Plaintiff and members of the Class were injured as a proximate cause or result of the Data Breach;

m. Whether Plaintiff and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and members of the Class;

n. Whether Defendant's practices and representations related to the Data Breach breached implied warranties;

o. What the proper measure of damages is; and

p. Whether Plaintiff and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

104. **Typicality.** Plaintiff's claims are typical of the claims of other members of the Class in that Plaintiff, and the members of the Class sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

105. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and Defendant has no defenses unique to Plaintiff.

106. **Superiority of Class Action**. A class action is also a fair and efficient method of adjudicating the controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

107. A class action is therefore superior to individual litigation because:

a. The amount of damages available to an individual plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. 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.

108. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

109. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

110. **Predominance**. Pursuant to Rule 23(b)(3), the issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include but are not limited to the questions identified above.

111. This proposed class action does not present any unique management difficulties.

112. **Injunctive Relief.** Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, provide proper notification to Class Members regarding the Data Breach, and conform its actions with applicable law as set forth in this Complaint.

113. **Issue Certification.** Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

f. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

114. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 113.

115. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

116. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to

third parties and by failing to properly supervise both the manner in which the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

117. Defendant owed Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary in order for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

118. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PII for rendering its services.

119. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

120. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

121. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiff's and members of the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the

Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

122. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and members of the Class's PII.

123. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, patients' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's sensitive PII.

124. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its patients in the event of a breach, which ultimately came to pass.

125. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

126. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

127. Defendant violated the Arizona Consumer Fraud Act (A.R.S. §§ 44-1521, *et seq*.) causing the Data Breach, a harm that the Arizona Consumer Fraud Act was intended to prevent.

128. Plaintiff and members of the Class are within the class of persons that the Arizona Consumer Fraud Act was intended to protect.

129. Defendant's violation of the Arizona Consumer Fraud Act constitutes negligence per se.

130. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

131. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

SECOND CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

133. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 113.

134. Plaintiff and members of the Class conferred a monetary benefit upon Defendant in the form of monies paid for services to Defendant's customers, a part of which was passed on to Defendant.

135. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to facilitate payment and services.

136. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class.

137. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference between the value of the benefits Plaintiff and Class Members conferred upon Defendant (monies paid and PII conferred) and the value of the unreasonable data privacy and security practices and procedures that they received.

138. Under principals of equity and good conscience, Defendant should not be permitted to retain the value belonging to Plaintiff and members of the Class because Defendant failed to implement (or adequately implement) the data privacy and security practices and procedures for itself that Plaintiff and members of the Class paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

139. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

THIRD CAUSE OF ACTION
Arizona Consumer Fraud Act,
A.R.S. §§ 44-1521, *et seq.*
(On Behalf of Plaintiff and the Class)

140. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 113.

141. Defendant sold "merchandise" as that term is defined by A.R.S. § 44-1521, in the form of goods and services, including information technology, marketing, and consulting services.

142. Section 44-1522 of the Arizona Consumer Fraud Act provides:

> The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

See A.R.S. § 44-1522(A).

143. Defendant used deception, used a deceptive act or practice, and fraudulently omitted and concealed material facts in connection with the sale or advertisement of that merchandise in violation of A.R.S. § 44-1522(A).

144. Defendant omitted and concealed material facts, which it knew about and had the duty to disclose—namely, Defendant's inadequate privacy and security protections for Plaintiff's and Class members' PII. Defendant omitted and concealed those material facts even though in equity and good conscience those facts should have been disclosed and did so with the intent that others would rely on the omission, suppression, and concealment.

145. The concealed facts are material in that they are logically related to the transactions at issue and rationally significant to the parties in view of the nature and circumstances of those transactions.

146. Defendant knew or should have known that its computer system and data security practices were inadequate to safeguard Plaintiff's and Class members' PII, and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in these deceptive acts and practices were negligent, knowing and willful, and wanton and reckless with respect to the rights of Plaintiff and Class members.

147. Specifically, Defendant failed to comply with the standards outlined by the FTC regarding protecting PII. As An information technology company, Defendant was or should have been aware of these standards. Defendant's data security systems did not

follow the FTC's guidelines and, as a result, were operating below the minimum standards set forth.

148. Plaintiff and Class members were ignorant of the truth and relied on the concealed facts and incurred damages as a consequent and proximate result.

149. Plaintiff and Class members seek all available relief under A.R.S. §§ 4421, *et seq.*, including, but not limited to, compensatory damages, punitive damages, injunctive relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, requests the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and the undersigned as Class counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures;

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. An award of damages, in an amount to be determined;

F. An award of attorneys' fees and costs;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

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

DEMAND FOR JURY TRIAL

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

Dated: January 31, 2023

Respectfully submitted,

/s/ Elaine A. Ryan
Elaine A. Ryan (AZ Bar #012870)
Colleen M. Auer (AZ Bar #014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
520-705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

Jean S. Martin*
Ra O. Amen*
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 223-5505
Facsimile: (813) 223-5402
JeanMartin@forthepeople.com
RAmen@forthepeople.com

*to seek admission *pro hac vice*

Counsel for the Plaintiff and the Proposed Class

ClassAction.org
