IN THE CIRCUIT COURT OF PULASKI COUNTY, ARKANSAS
_____ DIVISION

SAMUEL ACKER, PHILLIP DAVIDSON, and TERRY MORROW, individually, and on behalf of all others similarly situated, Plaintiffs, v. PROTECH SOLUTIONS, INC., Defendant.	Case No. Judge: **CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

Plaintiffs SAMUEL ACKER, PHILLIP DAVIDSON, and TERRY MORROW (collectively, "Plaintiffs"), by and through their attorneys, bring this class action lawsuit on behalf of themselves and all other persons similarly situated, and for their Class Action Complaint against Defendant PROTECH SOLUTIONS, INC., Plaintiffs allege with personal knowledge with respect to themselves individually and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters, as follows:

PARTIES

1. Plaintiff SAMUEL ACKER ("Acker") is a natural person with a principal place of residence in Cheyenne, Wyoming.

2. Plaintiff PHILLIP DAVIDSON ("Davidson") is a natural person with a principal place of residence in Paragould, Arkansas.

3. Plaintiff TERRY MORROW ("Morrow") is a natural person with a principal place of residence in Clarksville, Arkansas.

4. Defendant PROTECH SOLUTIONS, INC. ("Protech" or "Defendant") is an Arkansas corporation with a principal place of business in Little Rock, Arkansas.

JURISDICTION AND VENUE

5. Pursuant to Ark. Code Ann. § 16-4-101 and the due process of law clause of the Fourteenth Amendment of the United States Constitution, the Court has jurisdiction over PROTECH SOLUTIONS, INC. because it is an Arkansas corporation, has its headquarters in Arkansas, and regularly conducts business in Arkansas.

6. Venue lies in this Court pursuant to Ark. Code Ann. § 16-60-101 as a substantial part of the events or omissions that form the basis of this Class Action Complaint occurred in Pulaski County, Arkansas; Defendant conducted activity that gave rise to the claims for relief in this County; and Defendant maintains its headquarters in this County.

THE DATA BREACH

7. Plaintiffs bring this suit on behalf of themselves and a Class of similarly situated individuals against Defendant for Defendant's failure to secure and protect Plaintiffs' and Class members' personal and financial information.

8. Protech was hired by the state of Arkansas, to create, implement, and maintain a secure website for the Arkansas Division of Workforce Services ("ADWS") that would allow self-employed Arkansans and gig economy workers to apply online for unemployment benefits during the coronavirus pandemic, *i.e.*, the Pandemic Unemployment Assistance ("PUA") Application System. The contract between Arkansas and Protech provided that (i) Protech would be paid $3 million to create, implement, and maintain the PUA website, (ii) the website would be hosted on a secure/encrypted platform, and (iii) breaches would be able to be monitored to "protect the solution and the data within," such as social security numbers ("SSN") and banking information. The contract also required Protech to submit a data security plan that included automated notifications to the company and the State in the event of a breach.

9. Plaintiffs and Class members submitted PUA claims through the PUA Application System created, implemented, and powered by Protech. However, at one of the worst times in the lives of Plaintiffs and Class members, when they find themselves unemployed in the midst of a pandemic and resulting recession, Protech negligently and recklessly made Plaintiffs' and Class members' path to recovery significantly harder by interfering with their access to PUA payments and putting their identity and credit standing at risk.

10. Protech failed to create and implement a secure website for Plaintiffs and other Class members to submit claims for PUA benefits. As a result of Protech's actions and inactions, the social security numbers, birthdays, and banking information of approximately 30,000 PUA applicants have been exposed (the "Data Breach").

11. On May 15, 2020, the ADWS learned of the Data Breach and took the PUA Application System offline. On May 21, 2020, the ADWS notified Plaintiffs and Class members of the Data Breach, and informed Plaintiffs and Class members that they are eligible for complimentary credit monitoring and identity restoration services provided by MyIDCare™ powered by ID Experts, but only for a period of one year.

12. As a result of the Data Breach, the PUA Application System was temporarily shut down. Even after the PUA Application System was back up and running, Plaintiffs and other Class members were and are still locked out of their accounts pending a "fraud review."

13. As a result of the Data Breach, Plaintiffs and Class members must now be vigilant and review their credit reports for incidents of identity theft, and to educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

14. Data security breaches have dominated the headlines for the last two decades, and it does not take an IT industry expert to know that the failure to take reasonable security

precautions places individual's personal information at risk.

15. The general public can tell you the names of some of the biggest data breaches: Adobe, eBay, Equifax, LinkedIn, and Heartland Payment Systems, etc.[1]

16. Upon information and belief, Protech failed to use reasonable and necessary industry standards when creating, implementing, and maintaining the PUA Application System to prevent a data breach, including the FTC's guidelines, resulting in the Data Breach.

17. Likewise, Protech failed to create, implement, and maintain adequate safeguards for the online storage of personal and financial information of Plaintiffs and Class members, resulting in the Data Breach.

18. Because of its failure to create, maintain, and/or comply with necessary cybersecurity requirements, Protech was unable to ensure the protection of information security and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access to the personal and financial information, resulting in the Data Breach.

DAMAGES FROM DATA BREACHES

19. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[2]

---

[1] S*ee, e.g.*, Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Apr. 17, 2020), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html (last visited July 9, 2020).

[2] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," pg. 2, by U.S. Government Accountability Office, June 2007, at: https://www.gao.gov/new.items/d07737.pdf (last visited July 9, 2020) ("GAO Report").

20. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[3]

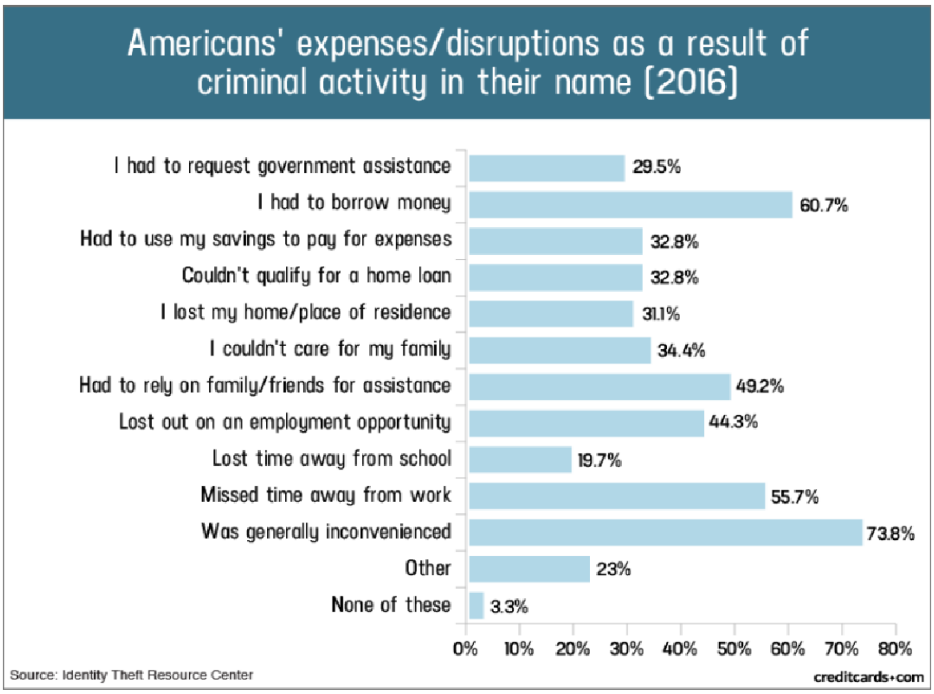
21. Identity thieves use stolen personal information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

22. Identity thieves can also use SSNs to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. When unemployment benefits are involved, some of the data entrusted to the Defendant included bank account numbers which, when used along with address and social security data, can be used to attempt to breach the bank accounts of the members of the Class compromising other money that those unemployment applicants might have in their accounts.

23. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:

---

[3] *See* https://www.identitytheft.gov/Steps (last visited July 20, 2020).



Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/17, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited July 9, 2020).

24. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

25. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

26. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, and are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

27. Data breaches are preventable.[4] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[5] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[6]

28. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[7]

FACTS RELEVANT TO PLAINTIFF SAMUEL ACKER

29. Acker is a citizen of Wyoming (and was during the period of the Data Breach).

30. Acker is disabled and, prior to the pandemic, Acker was a gig economy worker who worked as an independent contractor for an Arkansas company.

31. On or about May 5, 2020, Acker applied online for PUA benefits through the ADWS PUA Application System created, implemented, and maintained by Protech.

---

4 Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

5 *Id.* at 17.

6 *Id.* at 28.

7 *Id.*

32. As a direct result of the Data Breach, Acker did not receive a PUA payment until June 8, 2020. Further, Acker is now locked out of the PUA Application System and has not received a PUA payment since June 15, 2020, and he is unable to apply for further PUA benefits due to a "fraud review". As a direct result of the Data Breach, Acker has begun to face irreparable harms due to his inability to pay for his ongoing basic living expenses, such as the ability to purchase groceries and maintain current payments on his utility bills. As a direct result of the Data Breach, Acker has been unable to pay all of his bills, and has incurred penalties on his credit card accounts and other late fees.

33. As a direct result of the Data Breach, Acker will have to spend additional time and expend additional energy protecting and monitoring his identity and credit.

FACTS RELEVANT TO PLAINTIFF PHILLIP DAVIDSON

34. Davidson is a citizen of Arkansas (and was during the period of the Data Breach).

35. Prior to the pandemic, Davidson was self-employed and worked in Arkansas.

36. On or about May 5, 2020, Davidson applied online for PUA benefits through the ADWS PUA Application System created, implemented, and maintained by Protech.

37. As a direct result of the Data Breach, Davidson has not received a PUA payment since June 1, 2020, he has been unable to pay all of his bills, has fallen behind on his mortgage, and is now at risk of having his Chapter 13 bankruptcy (which he filed in March 2020), being dismissed for non-payment. Davidson has been locked out of the PUA Application System since June 1, 2020, and he has been unable to apply for further PUA benefits. Despite submitting various documents to prove his identity, Davidson continues to be locked out of the PUA Application System and is not receiving the PUA payments that he desperately needs. In addition to his Chapter 13 bankruptcy being in jeopardy of dismissal, the denial of access to PUA benefits has caused

Davidson the irreparable harm of not being able to afford his basic living expenses, including paying for groceries and maintaining current payments on his utilities.

38. As a direct result of the Data Breach, Davidson will have to expend additional time and energy protecting and monitoring his identity and credit.

FACTS RELEVANT TO PLAINTIFF TERRY MORROW

39. Morrow is a citizen of Arkansas (and was during the period of the Data Breach).

40. Prior to the pandemic, Morrow was self-employed before becoming unemployed, and he worked for Tyson Foods and Birchtree in Arkansas.

41. On or about May 14, 2020, Morrow applied online for PUA benefits through the ADWS PUA website created, implemented, and maintained by Protech. During the application process, Morrow supplied her account information for her Skylight Net Spin Card with Regions Bank, so that her PUA payments could be made directly to that account.

42. As a direct result of the Data Breach, Morrow was the victim of identity theft. The day after she applied online for PUA benefits through the PUA website created, implemented, and maintained by Protech, someone fraudulently used her name and SSN to set up an account with Bank of America in Texas ("BOA Account"), and without her authorization or knowledge transferred all her money from her Skylight Net Spin Card (*i.e.*, $757.24) into the BOA Account. Morrow spent approximately 20 hours trying to get her money back, including filing a police report and dealing with the bank. As a direct result of the data Breach, Morrow fell behind on paying her utilities and other bills. Morrow has also been charged late fees and penalties on accounts that, as a direct result of Defendant's conduct, have become delinquent.

43. As a direct result of the Data Breach, Morrow will have to expend additional time and energy protecting and monitoring her identity and credit.

PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

44. As a direct and proximate result of Protech's conduct, Plaintiffs and the Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

45. Plaintiffs and members of the Class have or will suffer actual injury as a direct result of the Data Breach including:

a. Loss of unemployment assistance payments for an extended period of time while the PUA Application System website was down and while their accounts are frozen for "fraud review";

b. Being unable to apply for an extension of PUA benefits due to their accounts being frozen for "fraud review", and spending time calling the hotline regarding the "fraud review";

c. The imposition of penalties, late fees, and other costs associated with their inability to obtain PUA benefits to pay their bills;

d. Spending time finding fraudulent charges and remedying fraudulent charges;

e. Damage to their credit;

f. Canceling compromised credit and debit cards and having them reissued;

g. Purchasing credit monitoring and identity theft prevention;

h. Time and money addressing and remedying identity theft;

i. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

j. Placing "freezes" and "alerts" with credit reporting agencies which, pursuant to Ark. Code Ann. § 4-112-111, will cost up to five dollars ($5.00) to place a security freeze on a credit report, to temporarily lift a security freeze on a credit report, or to remove a security freeze from a credit report;

k. Spending time on the phone with or visiting financial institutions to dispute fraudulent charges;

l. Contacting their financial institutions and closing or modifying financial accounts;

m. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

n. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

o. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

46. Moreover, Plaintiffs and the Class members have an interest in ensuring that their personal and financial information is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data containing their personal and financial information is not accessible online.

47. As a direct and proximate result of Protech's actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, loss of privacy, identity theft, financial damages, and are at an increased and immediate risk of future harm.

CLASS ALLEGATIONS

48. **Class Definition**: Plaintiffs bring this action pursuant to Ark. R. Civ. P. 23, on behalf of a class of similarly situated individuals and entities ("the Class"), defined as follows:

> All individuals who applied for Pandemic Unemployment Assistance ("PUA") with the Arkansas Division of Workforce Services through the PUA Application System designed, implemented, and maintained by Protech Solutions, and whose personal information and/or financial information was exposed in the Data Breach.
>
> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

49. **Numerosity**: Upon information and belief, the Class is comprised of tens of thousands of members. Initial reports state that approximately 30,000 Arkansans had sensitive and

confidential information exposed.[8] Thus, the Class is so numerous that joinder of all members is impracticable. Class members can easily be identified through records of the ADWS, or by other means.

50. **Commonality and Predominance**: There are several questions of law and fact common to the claims of Plaintiffs and Class members, which predominate over any individual issues, including:

a. Whether Protech created, implemented, an maintained the PUA Application System without adequate protections for the personal and financial information of Plaintiffs and members of the Class;

b. Whether Protech adopted, implemented, and maintained reasonable safeguards to prevent the unauthorized access to the personal and financial information of Plaintiffs and members of the Class;

c. Whether Protech promptly provided notification of the Data Breach;

d. Whether Protech owed a duty to Plaintiffs and members of the Class to safeguard and protect their personal and financial information;

e. Whether Protech breached a duty to Plaintiffs and members of the Class to safeguard and protect their personal and financial information;

f. Whether Protech breached a duty to Plaintiffs and members of the Class by failing to adopt, implement, and maintain reasonable safeguards to protect the personal and financial information of Plaintiffs and members of the Class; and

g. Whether Protech is liable for the damages suffered by Plaintiffs and members of the Class as a result of the Data Breach.

51. **Typicality**: Plaintiffs' claims are typical of the claims of members of the Class. All claims are based on the same legal and factual issues. Plaintiffs and each of the Class members

[8] *See* https://www.govtech.com/templates/gov_print_article?id=570572181 (last visited July 9, 2020) ("Arkansas was forced to temporarily shut down an unemployment benefits program last week after a data breach potentially exposed the personal information of some 30,000 state residents.").

provided their personal and financial information through the PUA Application System created, implemented, and maintained by Protech. Defendant's conduct was uniform to Plaintiffs and all Class members.

52. **Adequacy of Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class, and have retained counsel competent and experienced in complex class actions. Plaintiffs have no interests antagonistic to those of any members of the Class, and Defendant has no defenses unique to Plaintiffs. The questions of law and fact common to the proposed Class predominate over any questions affecting only individual members of the Class.

53. **Superiority**: A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually. The trial and the litigation of Plaintiffs' claims are manageable.

COUNT I
Negligence
(On behalf of Plaintiffs and the Class)

54. Plaintiffs repeat and reallege the allegations of paragraphs 1-53 with the same force and effect as though fully set forth herein.

55. Protech's actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiffs and Class members. Protech knew, or should have known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and Class members and the importance of adequate security in creating, implementing, and maintaining the PUA Application System. Indeed, the contract between ADWS and Protech

specifically addressed data security. Additionally, Protech was well aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

56. Protech had a common law duty to prevent foreseeable harm to those whose personal and financial information it was entrusted. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Protech to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal and financial information would not be unsecured and accessible by unauthorized persons. Protech knew that the PUA Application System was for the implementation and provision of services for the Coronavirus Aid, Relief, and Economic Security ("CARES") Act of 2020 Federal Pandemic Unemployment Assistance Program. Thus, Protech knew that Plaintiffs and Class members who would be applying for assistance under the PUA program are unemployed and have significant short-term economic need. Further, Protech knew that if the PUA Application System did not work correctly, had to be temporarily or permanently taken down, or applicants were locked out of the system, then Plaintiffs and Class members would be unable to obtain their PUA payments, which would detrimentally impact the applicants' ability to pay for basic living expenses or maintain current payments on utility or other bills.

57. Protech had a special relationship with Plaintiffs and Class members. By creating, implementing, and maintaining the PUA Application System, Protech was entrusted with Plaintiffs' and Class members' electronic data containing their personal and financial information, and Protech was in a position to protect the electronic data (and the personal and financial information) from unauthorized access.

58. The duties of Protech also arose under section 5 of the Federal Trade Commission Act ("FTC 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 individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Protech.

59. Protech had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal and financial information in its possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

60. More specifically, the duties of Protech included, among other things, the duty to:

a. Adopt, implement, and maintain adequate security measures for protecting an individual's personal and financial information to ensure that the information is not accessible online by unauthorized persons; and

b. Adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches.

61. Protech breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the electronic data containing an individual's personal and financial information in its possession on the PUA Application System so that the electronic data would not come within the possession, access, or control of unauthorized persons. For example, the experience of Morrow shows that Class members' personal and financial information is at risk of, and is actually, being accessed and misused by unauthorized third parties.

62. Protech acted with reckless disregard for the security of the personal and financial information of Plaintiffs and the Class because Protech knew or should have known that its data security for the PUA Application System was not adequate to safeguard the personal and financial information that was collected and stored.

63. Protech acted with reckless disregard for the rights of Plaintiffs and the Class by failing to promptly detect the Data Breach, and further, provide notice of the Data Breach pursuant

to Ark. Code Ann. § 4-110-105, so that Plaintiffs and Class members could take measures to protect themselves from damages caused by the unauthorized access to the personal and financial information compromised in the Data Breach.

64. As a result of the conduct of Protech, Plaintiffs and Class members have suffered and will continue to suffer foreseeable harm. Plaintiffs and Class members have suffered actual damages including, but not limited to, identify theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses, including loss of unemployment assistance for an extended period of time while their accounts are frozen for "fraud review."

COUNT II
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

65. Plaintiffs repeat and reallege the allegations of paragraphs 1-53 with the same force and effect as though fully set forth herein.

66. Defendant invaded the right to privacy of Plaintiffs and Class members by displaying, disclosing, and allowing unfettered access of their personal and financial information to unauthorized and unknown individuals, and by failing to employ reasonable and necessary safeguards to prevent unauthorized access to Plaintiffs' and Class members' personal and financial information.

67. Plaintiffs' and Class members' personal and financial information was held privately and confidentially by them and used only for legitimate personal and financial purposes.

They only entrusted their personal and financial information to third parties as necessary for legitimate purposes, and required the third parties to hold the personal and financial information in confidence at all times and protect it against unauthorized disclosures. Plaintiffs and Class members were reasonable in expecting Defendant to maintain the security and confidentiality of their personal and financial information.

68. Defendant's conduct was and is highly offensive to a reasonable person with ordinary sensibilities.

69. As a result of the conduct of Protech, Plaintiffs and Class members have suffered and will continue to suffer actual damages including, but not limited to, identify theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses, including loss of unemployment assistance for an extended period of time while their accounts are frozen for "fraud review."

COUNT III
Injunctive Relief
(On Behalf of Plaintiffs and the Class)

70. Plaintiffs repeat and reallege the allegations of paragraphs 1-53 with the same force and effect as though fully set forth herein.

71. Protech's ongoing and continuing wrongful conduct, including its failures to employ reasonably adequate security over Plaintiffs' and Class' members' personal and financial

information and failures to adequately remedy the effects of the Data Breach, has caused and will continue to cause Plaintiffs and Class members to suffer irreparable harm.

72. Plaintiffs and Class members are suffering irreparable harm because they are under "fraud review" as result of the Data Breach and, therefore, are not receiving their unemployment assistance payments they need to pay for basic necessities, such as mortgage payments, rent payments, car payments, utility bills, and groceries. The lack of PUA payments creates a hardship that interferes with Plaintiffs' and Class members' ability to make these payments.

73. Plaintiffs and Class members are also suffering other forms of irreparable harm, including but not limited to: fraudulent charges, fraudulent activity relating to opening new accounts for credit, damage to their credit, out-of-pocket expenses, the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

74. Such irreparable harm will not cease unless enjoined by the Court.

75. Plaintiffs and the Class are entitled to injunctive relief and other affirmative equitable relief requiring Defendant to restore Plaintiffs' and Class members' access to the PUA Application System so that Plaintiffs and Class members can receive their desperately needed unemployment assistance payments.

76. If the requested injunction is not issued, Plaintiffs and the Class will suffer and continue to suffer the irreparable injury as set forth above.

77. The hardship to Plaintiffs and Class members if the injunction was not to issue would be significant. Plaintiffs and Class members are unemployed and cannot pay for basic necessities, such as groceries.

78. The requested injunctive relief is in the public interest, as it will provide assurances and security to Plaintiffs and Class members who are already vulnerable and in need of assistance, and will facilitate the increased participation in the PUA program, which exists for the purpose of aiding Plaintiffs and the Class, as well as future applicants and the economy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs SAMUEL ACKER, PHILLIP DAVIDSON, and TERRY MORROW, individually, and on behalf of all others similarly situated, respectfully request that judgment be entered in their favor and against PROTECH SOLUTIONS, INC., as follows:

A. Finding that this action satisfies the prerequisites for maintenance as a class action, and certifying the Class defined herein;

B. Appointing Plaintiffs as representatives of the Class;

C. Appointing Plaintiffs' counsel as counsel for the Class;

D. Entering judgment in favor of Plaintiffs and the Class against Defendant;

E. Awarding Plaintiffs and Class members actual and punitive damages, and all other forms of available relief, as applicable;

F. Awarding Plaintiffs and the Class attorney's fees and costs, including interest thereon as allowed or required by law;

G. Entering an injunction to mandatorily enjoin Defendant to immediately restore Plaintiffs' and Class members' access to the PUA Application System; and

H. Granting all such further and other relief as the Court deems just and appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs SAMUEL ACKER, PHILLIP DAVIDSON, and TERRY MORROW, individually, and on behalf of all others similarly situated, hereby demand a trial by jury on all claims so triable.

Respectfully submitted,

/s/ Dustin McDaniel

Dustin McDaniel
MCDANIEL, WOLFF & BENCA, PLLC
1307 West 4th Street
Little Rock, Arkansas 72201
(501) 954-8000 telephone
dmcdaniel@mwbfirm.com

Marc E. Dann (*pro hac vice* anticipated)
Brian D. Flick (*pro hac vice* anticipated)
DANNLAW
P.O. Box 6031040
Cleveland, Ohio 44103
(216) 373-0539 telephone
(216) 373-0536 facsimile
notices@dannlaw.com

Thomas A. Zimmerman, Jr. (*pro hac vice* anticipated)
tom@attorneyzim.com
Sharon Harris (*pro hac vice* anticipated)
sharon@attorneyzim.com
ZIMMERMAN LAW OFFICES, P.C.
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
www.attorneyzim.com
firm@attorneyzim.com

Counsel for Plaintiffs and the putative Class