IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON
IN AND FOR THE COUNTY OF KING

CANDY MOLINARI and MIKHAIL KHOLYUSEV, CHRISTINA JACKSON on Behalf of Themselves and All Others Similarly Situated, Plaintiffs, v. WELFARE & PENSION ADMINISTRATION SERVICE, Inc., Defendant.	Case No.: 22-2-04023-8 SEA **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Candy Molinari, Mikhail Kholyusev, and Christina Jackson, ("Plaintiffs"), on behalf of themselves and all others similarly situated, by and through their undersigned counsel, bring this consolidated class action complaint against Defendant, Welfare & Pension Administration Service, Inc. ("WPAS" or "Defendant"), alleging the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiffs, which are alleged upon personal knowledge.

I. INTRODUCTION

1.1 WPAS's primary business is third-party administration services for multi-employer benefit plans, including the administration of medical claims for participants of health

benefit funds. WPAS is in possession of incredible amounts of personally identifying information ("PII") and personal health information ("PHI") belonging to its clients' members, the participants of the benefit plans.

1.2 After allowing cybercriminals to roam through and pillage undetected in its computer network for six days, on July 21, 2021, WPAS discovered that portions of its self-designed and minimally-protected computer network had been infected with malware which encrypted certain yet-unidentified data (the "Data Breach"). It took WPAS seven days for its investigation to confirm that the unidentified data may have been accessed or removed from WPAS's network. It took WPAS another four (4) months to identify the information that was potentially impacted and to whom that information related. Shockingly, it took WPAS another month to begin notifying some data owners, and then another six weeks to notify over 100,000 affected individuals. WPAS's delay in determining who had been impacted and alerting the impacted participants is alarming.

1.3 WPAS touts its in-house PII and PHI data processing systems and technology as a means to maximize efficiency and save time and costs using external software products.

1.4 On information and belief, these cost-savings caused WPAS to implement lax or non-existent cybersecurity protocols, leaving the PII and PHI stored on its systems an unguarded target for theft and misuse.

1.5 Indeed, cybercriminals were able to breach WPAS's databases undetected for an unknown amount of time and steal the PHI and PII stored on WPAS's systems, causing the plan participants lifelong harm as the breach includes information they cannot change, like dates of birth and Social Security numbers. It is unclear how long access was available to the intruders, as no mention was made by WPAS in its Notice about the timing of initial breach, only discovery of the breach.

1.6 WPAS failed to properly secure and safeguard Plaintiffs' and the Class's private information stored within Defendant's information network, including, without limitation, PII

and PHI, including full names, Social Security numbers, health insurance information, and medical treatment/diagnosis information ("PII and PHI" or "Private Information").

1.7 WPAS was able to confirm that folders containing Plaintiffs' and the Class's Private Information was accessed in the Data Breach by July 28, 2021.

1.8 Despite the theft of this highly sensitive PHI and PII and the serious, lifelong risks that result from the Data Breach, WPAS offered only 12 months of free credit monitoring services, which does not adequately address the identity theft threat that the Data Breach poses to the plan participants.

1.9 Further, WPAS did not "immediately" notify victims of the Data Breach that their PHI and PII had been compromised, violating Washington's breach notification law, and preventing Plaintiffs and the proposed Class from taking the earliest opportunity to proactively mitigate the Data Breach's impact on them.

1.10 WPAS eventually began notifying individuals that their data, including names, addresses, insurance information, and Social Security numbers, were compromised nearly five (5) months later, on December 20, 2021.[1]

1.11 As of the time WPAS filed its Data Breach Notification with the State of Washington on February 18, 2022, 103,557 Washington residents were known to be affected by the Data Breach.[2]

1.12 Defendant maintained the PII and PHI in a reckless manner. In particular, the PII and PHI was maintained on Defendant's network system in a condition vulnerable to cyberattacks.

1.13 Defendant exposed Plaintiffs and Class Members to harm by willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were

[1] *Welfare & Pension Administration Service, Inc. Provides Notice of Data Event*, https://www.nbc4i.com/business/press-releases/cision/20220218CL67468/welfare-pension-administration-service-inc-provides-notice-of-data-event/ (last visited March 15, 2022).

[2] *Washington State Office of the Attorney General – Data Breach Notifications*, https://www.atg.wa.gov/data-breach-notifications (last visited March 15, 2022)

protected against unauthorized intrusions; failing to disclose that it did not have adequately robust network systems and security practices in place to safeguard participants' PII and PHI; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt notice of the Data Breach.

1.14 In addition, Plaintiffs' and Class Members' Private Information – which was entrusted to Defendant – was compromised and unlawfully accessed due to the Data Breach.

1.15 Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct since the PII and PHI that Defendant collected and maintained is now in the hands of hackers.

1.16 With their information available to hackers, bad actors can harm Plaintiffs and Class Members in a variety of ways, including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

1.17 Participants who trusted WPAS to securely store their information have suffered injury and ascertainable losses in the form of the present and imminent threat of fraud and identity theft, out-of-pocket expenses and value of time reasonably incurred to remedy or mitigate the effects of the data breach, loss of value of their personal information, and loss of the benefit of their bargain.

1.18 Plaintiffs Candy Molinari ("Molinari"), Mikhail Kholyusev ("Kholyusev"), and Christina Jackson ("Jackson"), are each victims of the Data Breach, and bring this class action lawsuit on behalf of themselves and those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII and PHI that Defendant collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party.

1.19 Plaintiffs' claims are brought as a class action, pursuant to CR 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of tens of thousands of individuals for negligence, breach of implied contract, violation of the Washington Data Breach Disclosure Law, RCW § 19.255.010, violation of the Washington State Consumer Protection Act (RCW 19.86.010 et seq.), unjust enrichment, invasion of privacy, and breach of fiduciary duty.

II. PARTIES

2.1 Plaintiff Molinari is a natural person and citizen of Washington, residing in Brinnon, Washington, where she intends to remain. Molinari provided her PII and PHI to WPAS prior to the Data Breach, which remains entrusted with WPAS through the present. Her information has been compromised as a result of the Data Breach, as she confirmed with WPAS through its telephone number hotline in its Notice, resulting in fraud alerts on her financial accounts for suspicious charges to her credit cards, and further requiring her to expend significant time and effort in cancelling and locking her credit cards, and causing her anxiety, sleep disruption, stress and fear.

2.2 Plaintiff Kholyusev is a natural person and citizen of Washington, residing in the City of Seattle, where he intends to remain. Mr. Kholyusev's personal information, including social security number and financial data, was maintained by WPAS, prior to the 2021 data breach and remains entrusted with WPAS through the present. Mr. Kholyusev was notified of Defendant's Data Breach, in February 2022, and that his private information being compromised as a result.

2.3 Within the last approximately three months, Mr. Kholyusev experienced unusual activity on two separate credits cards, was the victim of Sim Card Hacking, and was subject to repeated attempts by wrongdoers seeking to gain access to his email.

2.4 Plaintiff Jackson is natural person and citizen of Washington, residing in the City of Vancouver, where she intends to remain. Ms. Jackson's personal information, including social security number and financial data, was maintained by WPAS prior to the 2021 data breach and

remains entrusted with WPAS through the present. Ms. Jackson was notified of Defendant's Data Breach, in February 2022, and of her private information being compromised as a result.

2.5 Plaintiff Jackson has received emails from cyberstalkers demanding her credit card information and threatening to expose her sensitive information if she does not provide it to them. Additionally, Ms. Jackson received two alerts about unauthorized attempts to open credit cards in her name. As a result, Ms. Jackson placed a freeze on her credit report.

2.6 Defendant WPAS is a Washington state corporation, with its principal place of business at 7525 SE 24th St #200, Mercer Island, Washington, 98040. WPAS is a corporation that provides administrative services, including accounting, coordinating meetings, processing health claims, health and welfare administration, collecting dues, administering pension/retirement plans, and record retention.

III. JURISDICTION & VENUE

3.1 Jurisdiction is proper in this Court under RCW § 2.08.010.

3.2 This Court has personal jurisdiction over WPAS because it is incorporated under the laws of the State of Washington and its principal place of business is in Washington State, such that WPAS is at home in the State of Washington. Further, this action arises from WPAS's acts or omissions in Washington State.

3.3 Venue is proper in this Court under RCW § 4.12.020(3) because King County is where the causes of action arose.

IV. FACTUAL ALLEGATIONS

WPAS

4.1 WPAS is a third-party administration firm that specializes in multi-employer benefit plan administration.

4.2 WPAS administers over 80 Taft-Hartley funds and Public Trust Funds. These clients include AGC-International Union of Operating Engineers Local 701 Trust Funds; Northwest Glass, Molders, Pottery, Plastics and Allied Workers Pension Trust; Locals 302 and 612 of the International Union of Operating Engineers Trust Funds; Northwest Ironworkers Trust

Funds; Automotive Machinists Pension Trust; Machinists Health and Welfare Trust Fund; Puget Sound Benefits Trust; Northwest Plumbing and Pipefitting Industry Health, Welfare and Vacation Trust; Puget Sound Electrical Workers Trust Funds; Northwest Employees Retirement Plan Trust Fund; Washington State Council of County and City Employees Health and Welfare Trust; Northwest I.A.M. Benefit Trust; Alaska Carpenters Trust Funds; Western Metal Industry Pension Fund; Cement Masons & Plasterers Trust Funds; Theatrical Stage Employees Health & Welfare Trust; Northwest Roofers & Employers Health & Security Trust Fund; Alaska Painters Trust Funds; Washington-Idaho Operating Engineers Trust Funds; and Idaho Operating Engineers-Employers Pension Trust Fund. WPAS's clients have hundreds of thousands of members.

4.3 WPAS is also a third-party administrator of online substance abuse programs through its subsidiary CleanWorkForce.com (CWF). CWF offers professionally managed drug and alcohol testing programs, immediate access to employee-compliance status, and eliminates the administrative burdens associated with internal management.[3] Alaska Construction Industry Substance Abuse Program is one of WPAS's clients for these services.

4.4 As a part of those administrative services, WPAS offers record retention services for all necessary files required to administer the various trusts, which includes electronic records retention, which is ostensibly "subject to significant security, encryption, and utilization review by WPAS . . . ."[4]

4.5 WPAS advertises that it is committed to providing superior, cost-efficient, third-party administration services and strives to enhance its information technology and communication network systems by utilizing the most current tools available to assist in providing outstanding service to the participants of every plan it administers.[5]

[3] https://www.wpas-inc.com/WPAS/services/cleanworkforce.php (last visited March 17, 2022).
[4] *Our Services – Systems & Technology*, https://www.wpas-inc.com/WPAS/services/systems.php (last visited March 15, 2022).
[5] https://www.wpas-inc.com/WPAS/services/adminservices.php (last visited March 17, 2022).

4.6 WPAS states its "goal is to create a state of the art, fully integrated benefit management platform that will meet the needs of our clients."[6]

4.7 WPAS provides customized website services for its clients, allowing participants to access their personal benefits through a secure login. Specifically, individuals can use WPAS's website services to access personal information, medical and dental claims, contact information, and dependent information, among other things.[7]

4.8 WPAS collects and stores PII and PHI from its clients' members, the participants in the funds and plans, as part of its administrative services.[8]

4.9 WPAS advertises that a majority of its data-processing systems are built in-house, allowing it to maximize efficiency with customization designed to meet the needs of both WPAS's clients and staff and to save significant time and material costs for custom programming that would be associated with using external software products.[9]

4.10 As part of its benefit plan administration, WPAS collects, stores, and maintains all the necessary files required in the administration of each Trust, including, but not limited to, benefit claims, records of employer contributions, correspondence with service providers and participants.[10]

4.11 In the ordinary course of administering the affairs of trusts, WPAS is entrusted with, collects, stores, and maintains participants' private information, including, but not limited to, name, Social Security number, health insurance information, and medical/health diagnosis information.

[6] https://www.wpas-inc.com/ (last visited March 17, 2022).
[7] https://www.wpas-inc.com/WPAS/services/websiteservices.php (last visited March 17, 2022).
[8] WPAS Data Breach Notice (the "Breach Notice"), accessible on the Washington State Office of the Attorney General website, https://www.atg.wa.gov/welfare-pension-administration-service-inc-wpas (last visited March 17, 2022) and attached hereto as **Exhibit 1**.
[9] https://www.wpas-inc.com/WPAS/services/systems.php (last visited March 17, 2022).
[10] *Id.*

4.12 WPAS provides online data access to its clients and other interested parties. WPAS claims "[a]ll access is subject to significant security, encryption, and utilization review by WPAS staff to help prevent abuse or fraud."[11]

4.13 By obtaining, collecting, using and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

4.14 Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI.

4.15 Plaintiffs and the Class Members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business and health purposes only, and to make only authorized disclosures of this information.

4.16 For environmental and cost reasons, WPAS has been moving towards storing these records electronically, which allows parties to access the information online.

4.17 WPAS acknowledged the inherent dangers of digital record retention with online access, claiming it implemented additional security, encryption, and utilization review procedures to accompany the electronic record retention system.

4.18 In addition, WPAS touts its privacy protection training and procedures, noting that all WPAS employees are trained to preserve protected health information in accordance with HIPAA and that WPAS keeps a HIPAA privacy officer and violation contact person for all Taft-Hartley Health Trusts.

4.19 Yet, WPAS failed to implement reasonable cybersecurity policies, adequately train its employees on those policies, or enforce the policies to protect plan participants' PHI and PII.

[11] *Id.*

WPAS Failed to Safeguard PII and PHI, Resulting in its Electronic Record Retention Services Being Breached

4.20 Plaintiffs Kholyusev, Jackson, and Molinari, and the proposed Class are current and former plan participants.

4.21 In order to administer the funds and programs, WPAS requires plan participants to provide their PII and PHI, including their name, address, date of birth, Social Security number, driver's license or state identification number, financial account information, passport number, medical treatment and/or diagnosis information, and health insurance number.

4.22 WPAS collects and maintains plan participants' PII and PHI in its in-house computer systems.

4.23 In collecting and maintaining the PII and PHI, WPAS implicitly agrees to safeguard the data according to its internal policies and state and federal law.

4.24 Despite WPAS's promises to safeguard the PII and PHI it maintains, on July 21, 2021, WPAS discovered cybercriminals had bypassed WPAS's lax and outdated security safeguards and accessed and removed certain folders containing PII and PHI of its clients' members.

4.25 WPAS reported that the Data Breach began on July 15, 2021.[12] WPAS allowed the cybercriminals to pilfer PHI and PII undetected for six days before it realized a breach had occurred.

4.26 On information and belief, the Data Breach exposed the PII and PHI of over 280,000 individuals.

4.27 According to its Breach Notice, WPAS's computer network was infected with malware that encrypted yet-unidentified folders of data. The cybercriminals were able to access or remove these folders of data from WPAS's network.

4.28 By September 17, 2021 WPAS determined, at a minimum, certain folders containing data related to plan participants, including "name, Social Security number, health

[12] https://www.atg.wa.gov/welfare-pension-administration-service-inc-wpas (last visited March 18, 2022).

insurance information, and medical treatment/diagnosis information" were part of the data breach.

4.29 WPAS concluded its review of the breach on December 7, 2021, almost five months after the discovery of the breach—that the "lengthy, time-intensive, and thorough review of the affected folders" confirmed that the impacted data included certain plan participants' information. WPAS then began compiling information to contact participants who were potentially affected by the Data Breach.

4.30 After another thirteen (13) days, by December 20, 2021, WPAS completed its information compiling to confirm the accuracy of the impacted data and address information for impacted individuals and to identify the applicable WPAS clients and began the process of reaching out to potentially affected participants.

4.31 Despite this "comprehensive" and "thorough" investigation, WPAS still has not disclosed what information was taken for which participants, only that "potentially impacted information" could include name, address, date of birth, Social Security number, driver's license or state identification number, financial account information, passport number, medical treatment and/or diagnosis information, and health insurance numbers.[13]

4.32 WPAS did not start notifying "data owners" of the Data Breach until January 3, 2022.

4.33 It is unclear who WPAS notified at this time, because on February 18, 2022, WPAS received "additional information from clients" such that WPAS began providing written notice of the Data Breach to at least 103,557 Washington residents.[14]

4.34 WPAS also waited until February 18, 2022 to send out notice of the data breach to various government and news agencies.

4.35 At least 22 of the funds that WPAS administers were impacted by the Data Breach, including AGC-International Union of Operating Engineers Local 701 Trust Funds;

[13] *Id*.
[14] *Id*.

Northwest Glass, Molders, Pottery, Plastics and Allied Workers Pension Trust; Locals 302 and 612 of the International Union of Operating Engineers Trust Funds; Northwest Ironworkers Trust Funds; Automotive Machinists Pension Trust; Machinists Health and Welfare Trust Fund; Puget Sound Benefits Trust; Northwest Plumbing and Pipefitting Industry Health, Welfare and Vacation Trust; Puget Sound Electrical Workers Trust Funds; Northwest Employees Retirement Plan Trust Fund; Washington State Council of County and City Employees Health and Welfare Trust; Northwest I.A.M. Benefit Trust; Alaska Carpenters Trust Funds; Western Metal Industry Pension Fund; Cement Masons & Plasterers Trust Funds; Theatrical Stage Employees Health & Welfare Trust; Northwest Roofers & Employers Health & Security Trust Fund; Alaska Painters Trust Funds; Washington-Idaho Operating Engineers Trust Funds; Idaho Operating Engineers-Employers Pension Trust Fund; and Alaska Construction Industry Substance Abuse Program.

4.36 On information and belief, WPAS also exposed its own employees' PII and PHI in the Data Breach. WPAS required its employees to provide their PII and PHI as a requirement of employment and to administer their health benefits.

4.37 WPAS has not disclosed how the Data Breach happened, why WPAS was delayed in detecting the hack, how WPAS ended the hack, or whether WPAS has eliminated the security vulnerabilities that led to the Data Breach.

4.38 In other words, WPAS had no effective means to prevent, detect, stop, and mitigate the effects of the Data Breach before criminals successfully stole its participants' PHI and PII, including their names, dates of birth, and Social Security numbers. Further, WPAS has been unwilling or unable to disclose the details of how the breach occurred.

4.39 After the Data Breach was discovered, WPAS had ineffective means of identifying the damage caused by the Data Breach, the parties effected, and ineffective means of notifying impacted parties and governments.

4.40 Despite the lifelong harm that victims of the Data Breach face, WPAS offered them only 12 months of free credit monitoring,[15] which does not adequately address the costs the Data Breach will impose on them.

4.41 As evidence of this, WPAS reported the Data Breach to the U.S. Department of Health and Human Services Office for Civil Rights on September 17, 2021, claiming 545 individuals had been affected. Yet, by February 18, 2022, when WPAS reported the Data Breach to the Washington State Attorney General's Office, the number of affected individuals had grown to over 103,000 affected individuals.

4.42 WPAS states that it "continues to assess the security of WPAS systems and to enhance existing policies and procedures, including implementing additional safeguards intended to safeguard information and to reduce the likelihood of similar events."

4.43 On information and belief, WPAS allowed the Data Breach to occur because it failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over participants' PHI and PII. WPAS's negligence is evidenced by its failure to prevent the Data Breach, its inability to quickly detect the Data Breach, and its failure to stop cybercriminals from accessing Plaintiffs and Class members' PHI and PII. Further, the Breach Notice makes clear that WPAS cannot, or will not, determine the full scope of the Data Breach, as it has been unable to determine exactly how the breach occurred and has not identified any steps it is taking to prevent future breaches.

Plaintiffs' Experiences

4.44 Plaintiffs, Molinari, Kholyusev, and Jackson are each current participants of one of WPAS's clients.

4.45 Plaintiffs provided their PII and PHI to WPAS with the understanding that the company would use reasonable measures to protect it according to WPAS's internal policies and state and federal law.

[15] *Id*.

4.46 Plaintiffs' and Class members' expectation that WPAS would protect the security of the PII and PHI entrusted to it was reasonable in light of WPAS's status as a fiduciary of the funds and the claimed protections on their website.

4.47 Plaintiff Kholyusev was notified of Defendant's Data Breach in February 2022 and that his private information was compromised and released by WPAS to unauthorized persons as a result.

4.48 Thereafter, Plaintiff Kholyusev experienced unusual activity on two separate credits cards, fell victim to a Sim Card Hacking, and he was the target of repeated attempts by wrongdoers seeking to gain access to his email. Plaintifff Kholyusev has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Kholyusev fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

4.49 Plaintiff Jackson was notified of Defendant's Data Breach in February 2022 and that her private information was compromised and released by WPAS to unauthorized persons as a result.

4.50 Plaintiff Jackson has received emails from cyberstalkers demanding her credit card information and threatening to expose her sensitive information if she does not provide it to them. Additionally, Ms. Jackson received two alerts about unauthorized attempts to open credit cards in her name. As a result, Ms. Jackson placed a freeze on her credit report. Plaintiff Jackson has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Jackson fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

4.51 Plaintiff Molinari did not receive WPAS's mailed Breach Notice, but confirmed via WPAS's toll-free data breach telephone number that her private information was compromised and released by WPAS to unauthorized persons as a result.

4.52 In early March 2022, Plaintiff Molinari received two fraud alerts from Capital One Bank and Bank of America for suspicious and excessive charges made on her credit cards. She has spent hours cancelling and locking her credit cards and ordering new ones.

4.53 Plaintiff Molinari has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Molinari fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Molinari has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

4.54 Plaintiffs and members of the proposed Class have suffered injury from the unauthorized access to and misuse of their PII and PHI that can be directly traced to Defendant.

4.55 As a result of WPAS's failure to prevent the Data Breach, Plaintiffs 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 and PHI are used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

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 PHI; and

h. The continued risk to their PII and PHI, 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 it.

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

4.57 The value of Plaintiffs and the proposed Class's PII and PHI 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.

4.58 In fact, the value of this highly sensitive PII and PHI is precisely why cybercriminals targeted and stole it.

4.59 It can take victims years to spot fraud or identity theft, giving criminals plenty of time to convert the stolen PII and PHI for cash.

4.60 One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.

4.61 Cyber-criminals can cross-reference multiple sources of PII and PHI 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.

4.62 The development of "Fullz" packages means that stolen PII and PHI from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class members' 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 and PHI 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 Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

4.63 Defendant disclosed the PII and PHI of Plaintiffs 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 and PHI of Plaintiffs 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 and PHI.

4.64 Defendant's failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

4.65 Further, the way WPAS responded to the Data Breach increased the risk of harm to Plaintiffs and the Class.

4.66 WPAS waited an extraordinary amount of time to alert affected participants, with some participants not being alerted for at least five months from when WPAS recognized that Private Information had been accessed, enhancing the danger to Plaintiffs and Class Members.

4.67 From the time WPAS determined that a data breach had taken place, it took only a week to identify that some folders had been accessed or removed.

4.68 At the Plaintiffs' and Class's expense, it took an additional month and a half for WPAS to determine that some of its participants' Private Information was exposed in the Data Breach, and more than three (3) additional months to start sending out notices.

4.69 WPAS's own ineffective efforts to ameliorate the damage caused by failing to secure Plaintiffs' and the Class's Private Information culminated in the offer of inadequate credit monitoring services.

Defendant Had an Obligation to Protect PII and PHI Under Federal Law and the Applicable Standard of Care

4.70 The HIPAA Privacy Rule (45 CFR, Parts 160 and 164(A) and (E), among other sections, hereinafter "HIPAA") establishes national minimum standards for the protection of individuals' medical records and other personal health information. HIPAA sets minimum standards for Defendant's maintenance of Plaintiffs' and Class members' personal and medical information. More specifically, HIPAA requires appropriate safeguards be maintained to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without authorization. HIPAA also establishes individuals' rights over their health information, including rights to examine and obtain copies of their health records, and to request corrections thereto.

4.71 Additionally, the HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

4.72 HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

4.73 HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected

health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

4.74 Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414 requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

4.75 By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' PII and PHI, Defendant assumed legal and equitable duties to those individuals. In fact, Defendant states on its website that "WPAS, Inc. is currently in compliance with all HIPAA EDI Privacy and Security requirements."

4.76 Defendant violated its duty to Plaintiffs and Class Members through its failure to protect against a foreseeable cyber-attack.

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

4.78 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. Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

4.79 The FTC recommends that companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

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

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

4.81 By negligently securing Plaintiffs' and Class members' PII/PHI and allowing an unknown third-party cybercriminal to access Defendant's unencrypted, unprotected PII and PHI, Defendant failed to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data. Defendant's data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

V. CLASS ACTION ALLEGATIONS

5.01 Plaintiffs Molinari, Kholyusev, and Jackson sue on behalf of themselves and the class ("Class"), defined as follows:

> All Washington citizens who participated in funds or trusts managed by WPAS, whose PII and/or PHI was compromised as a result of the Data Breach.

5.02 Excluded from the Class are Defendant, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

5.03 Plaintiffs reserve the right to amend the Class definition above if further investigation and/or discovery reveals that the Class should be expanded, narrowed, divided into subclasses, or otherwise modified in any way.

5.04 This action satisfies the numerosity, commonality, typicality, and adequacy requirements under CR 23.

5.05 **Numerosity, CR 23(a)(1):** Plaintiffs are representative of the proposed Class consisting, upon information and belief, of over 100,000 members—far too many to join in a single action, and so numerous that joinder of all Class members is impracticable. Although the precise number of such persons is unknown, and the facts are presently within the sole knowledge of Defendant, WPAS.

5.06 **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control.

5.07 **Commonality, CR 23(a)(2):** Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

a. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII and PHI;
b. 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;
c. Whether Defendant was negligent in maintaining, protecting, and securing PII and PHI;
d. Whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's PII and PHI;
e. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;
f. Whether Defendant's Breach Notice was reasonable;
g. Whether the Data Breach caused Plaintiffs and the Class injuries;
h. What the proper damages measure is;
i. Whether Defendant violated the statutes alleged in this complaint; and

j. Whether Plaintiffs and the Class are entitled to damages, treble damages, or injunctive relief.

5.08 **Typicality, CR 23(a)(3)**: Plaintiffs' claims are typical of Class member's claims. Plaintiffs, like the other participants of funds or trusts managed by WPAS, have been subjected to WPAS's inadequate handling of their PII, resulting in the Data Breach, the same alleged negligence, contract, and statutory violations by Defendant, the same unreasonable manner of notifying individuals about the Data Breach; further, the injury and harm suffered by Plaintiffs is similar to that suffered by all other Class members, caused by the same misconduct by WPAS.

5.09 **Adequacy of Representation, CR 23(a)(4):** Plaintiffs will fairly and adequately protect the proposed Class's interests. Their interests do not conflict with and are not antagonistic to the Class members' interests, and Plaintiffs have retained competent counsel experienced in complex class action and data privacy litigation to prosecute this action vigorously on the Class's behalf, including as lead counsel.

5.10 **Predominance and Superiority, CR 23(b)(3):** Plaintiffs also satisfies the requirements under CR 23(b)(3). Common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

VI. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF

Negligence

(On behalf of Plaintiffs and the Proposed Class)

6.1 Plaintiffs reallege all previous paragraphs as if fully set forth below.

6.2 Plaintiffs and members of the Class entrusted their PII and PHI to Defendant. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII and PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect, secure and safeguard the Private

information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties, as transpired in the Data Breach, and to promptly detect attempts at unauthorized access.

6.3 Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that its failure to adequately safeguard their PII and PHI in accordance with state-of-the-art industry standards concerning data security, and the applicable standards of care from statutory authority like HIPAA and Section 5 of the FTC Act, would result in the compromise of that PII and PHI—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII and PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

6.4 Further, Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its plan participants, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. WPAS was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach. Plaintiffs and Class members reasonably believed that Defendant would take adequate security precautions to protect their Private Information.

6.5 Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

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

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

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

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

6.9 Defendant owed these duties to Plaintiffs 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 Plaintiffs' and members of the Class's PII and PHI.

6.10 The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant holds vast amounts of PII and PHI, it was "inevitable" that unauthorized individuals would attempt to access Defendant's databases containing the PII and PHI—whether by malware or otherwise.

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

6.12 Defendant breached its duties of care owed to the Plaintiffs and the Class Members by failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; by failing to adequately monitor the security of its

networks and systems; and by failing to periodically ensure that its computer systems and networks had plans in place to maintain reasonable data security safeguards.

6.13 Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' Private Information.

6.14 Moreover, Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the PII and PHI of Plaintiff and members of the Class which actually and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury.

6.15 Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs 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.

6.16 Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII and PHI by criminals, improper and unauthorized disclosure of their PII and PHI, lost benefit of their bargain, lost value of their PII and PHI, 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.

6.17 As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members regarding what type of PII and PHI had been compromised, Plaintiffs and Class Members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

6.18 Defendant's breaches of duty caused Plaintiffs and Class Members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their PII and PHI.

6.19 As a result of Defendant's negligence and breach of duties, Plaintiffs and Class Members are in danger of imminent harm in that their PII and PHI, which is still in the possession of third parties, and will be used for fraudulent purposes.

6.20 Plaintiffs seek the award of actual damages on behalf of the Class, to compensate them for the harm caused by the Data Breach, resulting directly from Defendant's negligence as set forth herein.

SECOND CLAIM FOR RELIEF

Breach of an Implied Contract

(On behalf of Plaintiffs and the Proposed Class)

7.1 Plaintiffs incorporate the above allegations as if fully set forth herein.

7.2 Defendant required Plaintiffs and members of the Class to entrust it with their PII and PHI in order to administer their health benefit plans and other programs.

7.3 In turn, and through internal policies, Defendant agreed it would safeguard and not disclose the PII and PHI it collects to unauthorized persons.

7.4 Plaintiffs and the members of the Class accepted Defendant's offer by providing PII and PHI to Defendant in exchange Defendant's services.

7.5 Implicit in the parties' agreement was that Defendant would adequately safeguard the PII and PHI entrusted to and would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII and PHI.

7.6 Plaintiffs and the members of the Class would not have entrusted their PII and PHI to Defendant in the absence of such agreement with Defendant.

7.7 Defendant materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them

promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiffs and members of the Class by:

A. Failing to properly safeguard and protect Plaintiffs' and members of the Class's PII and PHI;

B. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

C. Failing to ensure the confidentiality and integrity of electronic PII and PHI that Defendant created, received, maintained, and transmitted.

7.8 The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

7.9 Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

7.10 The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

7.11 Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

7.12 Defendant knew or should have known that Plaintiffs and Class members reasonably understood that Defendant would safeguard the PII and PHI Defendant required Plaintiffs and Class members to disclose in order for Defendant to do its job and administer their health plans. Despite Plaintiffs' and Class members' reasonable expectations, Defendant failed to

implement appropriate cybersecurity protocols to protect the PII and PHI on its systems from the Data Breach.

7.13 Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

7.14 In these and other ways, Defendant violated its duty of good faith and fair dealing.

7.15 Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

THIRD CLAIM FOR RELIEF

Violation of the Washington Data Breach Disclosure Law

(On Behalf of Plaintiffs and the Proposed Class)

8.1 Plaintiffs incorporate all previous paragraphs as if fully set forth below.

8.2 RCW § 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

8.3 The Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

8.4 Defendant failed to disclose that the PII and PHI of thousands of current and former members of clients had been compromised "immediately" upon discovery, and in doing so unreasonably delayed informing Plaintiff and the proposed Class about the Data Breach.

8.5 Plaintiffs and the proposed Class were damaged as a direct and proximate result of Defendant's failure to provide timely notice.

FOURTH CLAIM FOR RELIEF

Violation of the Washington State Consumer Protection Act (RCW 19.86.010 *et seq.*)

(On Behalf Of Plaintiffs And All Class Members)

9.1 Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

9.2 The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

9.3 Defendant is a "person" as described in RWC 19.86.010(1).

9.4 Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

9.5 By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

9.6 In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

9.7 Defendant also violated the CPA by failing to timely notify and concealing from Plaintiffs and Class Members the unauthorized release and disclosure of their PII/PHI. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII/PHI, medical information, and identities.

9.8 Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

9.9 The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

9.10 As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud; (2) invasion of privacy; (3) breach of the confidentiality of his other PII/PHI; (5) deprivation of the value of his or her PII/PHI, for which there is a well-established national and international market; and/or (v) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

9.11 Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class Members, and the general public, also seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage,

monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII/PHI entrusted to it.

9.12 Plaintiffs, on behalf of themselves and the Class Members also seek to recover actual damages sustained by each class member together with the costs of the suit, including reasonable attorney fees. In addition, the Plaintiffs, on behalf of themselves and the Class Members request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each class member by three times the actual damages sustained not to exceed $25,000.00 per class member.

FIFTH CLAIM FOR RELIEF

Unjust Enrichment

(On Behalf of Plaintiffs and the Proposed Class)

10.1 Plaintiffs incorporate the above allegations as if fully set forth herein.

10.2 This claim is pleaded in the alternative to the breach of implied contractual duty claim.

10.3 Plaintiffs and members of the Class conferred a benefit upon Defendant by paying for Defendant's administration services.

10.4 Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendant also benefited from the receipt of Plaintiffs and members of the Class's PII and PHI, as this was used for Defendant to administer its clients' funds and programs.

10.5 Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the proposed Class's services and their PII and PHI because Defendant failed to adequately protect their PII and PHI. Plaintiffs and the proposed Class would not have provided their PII and PHI or paid the fee to Defendant for its administration services had they known Defendant would not adequately protect their PII and PHI.

10.6 Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

SIXTH CLAIM FOR RELIEF
Invasion of Privacy

(On Behalf of the Plaintiff and Proposed Class)

11.1. Plaintiffs incorporate all previous paragraphs as if fully set forth below.

11.2. Defendant publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiffs and Class members by disclosing and exposing Plaintiffs' and Class Members' private and sensitive PHI and PII to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

11.3. Plaintiffs' and Class Members' PHI and PII, which included their names, addresses, dates of birth, Social Security numbers, driver's license or state identification numbers, financial account information, passport numbers, medical treatment and/or diagnosis information, and health insurance numbers, was private and intimate.

11.4. Defendant's disclosure of the PHI and PII unreasonably, substantially and seriously interfered with Plaintiffs' and Class Members' privacy and ordinary sensibilities. Defendant should appreciate that the cyber-criminals who stole the PHI and PII would further sell and disclose it as they are doing and as they did. That the original disclosure is devastating to Plaintiffs and Class Members even though it may have originally only been made to one person or a limited number of cyber-criminals does not render it any less a disclosure to the public-at-large.

11.5. The tort of public disclosure of private facts is recognized in Washington. Plaintiffs' and Class Members' private and sensitive PHI and PII was publicly disclosed by

Defendant in the Data Breach with reckless disregard for the offensiveness of the disclosure. Such disclosure is highly offensive and would be to any person of ordinary sensibilities. Defendant knew that Plaintiffs' and Class Members' PHI and PII is not a matter of legitimate public concern. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been injured and are entitled to damages.

SEVENTH CLAIM FOR RELIEF

Breach of Fiduciary Duty

(On Behalf of Plaintiffs and All Class Members)

12.1 Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

12.2 In light of its special relationship to Plaintiffs and Class Members as plan participants, Defendant became the guardian of Plaintiffs' and Class Members' PII and PHI. Defendant became a fiduciary, created by its undertaking and guardianship of its plan participants' PII and PHI, to act primarily for the benefit of those individuals, including Plaintiffs and Class Members. This duty included the obligation to safeguard Plaintiffs' and Class Members' PII and PHI and to timely detect and notify them in the event of a data breach.

12.3 Defendant knowingly undertook the responsibility and duties related to the possession of Plaintiffs' and Class Members' PII/PHI for the benefit of Plaintiffs and Class Members in order to provide them with its services.

12.4 Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with them. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to properly encrypt and otherwise protect their PII and PHI. Defendant further breached its fiduciary duties owed to

Plaintiffs and Class Members by failing to timely detect the Data Breach and notify and/or warn Plaintiffs and Class Members of the Data Breach.

12.5 As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered or will suffer concrete injury, including but not limited to (a) actual identity theft; (b) the loss of the opportunity of how their PII and PHI is used; (c) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PII and PHI; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII and PHI; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their PII and PHI, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII and PHI in its continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a direct and traceable result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

12.6 As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

VII. PRAYER FOR RELIEF

Plaintiffs, Candy Molinari, Mikhail Kholyusev, and Christina Jackson and the members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about its data security, the Data Breach, and the stolen PII and PHI;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

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

J. Granting such other or further relief as may be appropriate under the circumstances.

VIII. JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 15th day of July, 2022.

DATED: July 15, 2022

SMITH & DIETRICH LAW OFFICES PLLC

By: s/ *Walter Smith*
Walter Smith, WSBA #46695
3905 Martin Way E., Suite F
Olympia, WA 98506
Telephone: (360) 915-6952
Email: walter@smithdietrich.com

BADGLEY MULLINS TURNER PLLC
Duncan C. Turner, WSBA #20597
19929 Ballinger Way, Suite 200
Seattle, WA 98155
Telephone: 206-621-6566
Facsimile: 206-621-9686
Email: dturner@badgleymullins.com

LEVI & KORSINSKY, LLP
Mark S. Reich (admitted *pro hac vice* in *Kholyusev* case prior to consolidation)
Courtney E. Maccarone (admitted *pro hac vice* in *Kholyusev* case prior to consolidation)
55 Broadway, 10th Floor
New York, NY 10006
Telephone: 212-363-7500
Facsimile: 212-363-7171
Email: mreich@zlk.com
cmaccarone@zlk.com

TURKE & STRAUSS LLP
Samuel J. Strauss, WSBA #46971
936 North 34th Street, Suite 300
Seattle, Washington 98103-8869
Telephone: (608) 237-1775
Email: sam@turkestrauss.com

BRANSTETTER, STRANCH & JENNINGS, PLLC
J. Gerard Stranch, IV (*pro hac vice*)
Peter J. Jannace (*pro hac vice*)
223 Rosa L. Parks Avenue, Suite 200
Nashville, TN 37203
Telephone: (615) 254-8801
Email: gerards@bsjfirm.com
peterj@bsjfirm.com

Counsel for Plaintiffs