

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26

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

GARY STEVE CLOPP, SHLON SMITHSON,  
and LEEANN CRAWFORD, individually and  
on behalf of all others similarly situated,

No. 21-2-08738-4 KNT

CLASS ACTION COMPLAINT FOR:

Plaintiffs,

1. Negligence
2. Violation of the Washington  
Consumer Protection Act, RCW §  
19.86, *et seq.*

v.

PACIFIC MARKET RESEARCH, LLC, a  
Washington limited liability company; and  
DOES 1-20,

Defendants.

Plaintiffs Gary Steve Clopp, Shlon Smithson, and LeeAnn Crawford (collectively, “Plaintiffs”), by and through their counsel, bring this Class Action Complaint against Defendant Pacific Market Research, LLC, a Washington limited liability company (“Defendant” or “PMR”) on behalf of themselves and all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel’s investigations, and upon information and belief as to all other matters, as follows:

**I. INTRODUCTION**

1. Plaintiffs bring this class action lawsuit on their own behalf, and on behalf of a Class of similarly situated individuals (the “Class”), against Defendant for its failure to protect the sensitive, confidential information of individuals in the state of Washington—including such

1 information as the person's name, address, telephone number, social security number, workers'  
2 compensation claim number(s), date of birth, and medical information ("Personal Information"  
3 or "PI").

4 2. The Office of the Washington Department of Labor & Industries ("L&I") recently  
5 publicly admitted that sensitive information of 16,466 individuals in the State of Washington was  
6 compromised in a data security breach of its customer service survey contractor, Pacific Market  
7 Research." A true and correct copy of L&I's press release dated July 1, 2021 is attached hereto  
8 as Exhibit 1 and incorporated herein by reference.

## 9 II. PARTIES

10 3. Paragraphs 1 – 2 are incorporated herein by reference.

11 4. Plaintiff Gary Steve Clopp ("Mr. Clopp") is an individual and is a resident of Lake  
12 Stevens, Snohomish County, Washington. Mr. Clopp filed for workers' compensation benefits  
13 with the State of Washington.

14 5. Plaintiff Shlon Smithson ("Ms. Smithson") is an individual and is a resident of  
15 Shelton, Mason County, Washington. Ms. Smithson filed for workers' compensation benefits  
16 with the State of Washington.

17 6. Plaintiff LeeAnn Crawford ("Ms. Crawford") is an individual and is a resident of  
18 Snohomish, Snohomish County, Washington. Ms. Crawford filed for workers' compensation  
19 benefits with the State of Washington.

20 7. Defendant Pacific Market Research, LLC is a Washington limited liability  
21 company and is headquartered at 15 S Grady Way, Suite 620, Renton, WA 98057.

## 22 III. JURISDICTION AND VENUE

23 8. Paragraphs 1 – 7 are incorporated herein by reference.

24 9. Jurisdiction is appropriate in this Court pursuant to RCW 2.08.010.  
25  
26

1           10.     This Court has personal jurisdiction over Defendant because Defendant’s principal  
2 place of business is in Washington State, Defendant regularly transacts business in Washington,  
3 and the events that give rise to Plaintiffs’ claims occurred in Washington.

4           11.     Venue is proper in this Court pursuant to RCW 4.12.020 and/or RCW 4.12.025  
5 because the acts and omissions alleged herein took place in whole or in part in King County,  
6 Washington and the Defendant resides and transacts business in King County, Washington.

7           12.     Federal jurisdiction is inappropriate under the Class Action Fairness Act, 28  
8 U.S.C. § 1332(d)(4)(A), because: (a) all members of the Class are residents of Washington, or  
9 were residents of Washington, at all times relevant to their employment with Defendant.  
10 Additionally: (b) Defendant is registered to conduct business, and regularly transacts business,  
11 within the State of Washington; (c) the alleged conduct of Defendant occurred within  
12 Washington; (d) the injuries to Plaintiff and the Class occurred within Washington; and (e)  
13 during the three-year period preceding the filing of this action, no other class action has been  
14 filed asserting the same or similar factual allegations against Defendant on behalf of the same  
15 persons. Alternatively, federal jurisdiction is inappropriate under the Class Action Fairness Act,  
16 28 U.S.C. § 1332 (d)(4)(B), because the members of the Class all reside in Washington.

17                                   **IV. FACTUAL BACKGROUND**

18           **The Defendant, Pacific Market Research**

19           13.     Paragraphs 1 – 12 are incorporated herein by reference.

20           14.     Defendant PMR advertises itself as “the largest data collection firm in the Pacific  
21 Northwest.”

22           15.     Defendant advertises that it is “among a handful of firms approved for high  
23 government projects, allowing us to handle . . . secure data.”

24           16.     In contrast to its advertised statements, Defendant’s systems are inadequate to  
25 protect the sensitive data it receives from its clients, and Defendant knew, or should have known,  
26

1 that it was highly vulnerable to a data breach, and that any sensitive information in its possession  
2 was insecure.

### 3 **The Data Breach**

4 17. Unbeknownst to Plaintiffs, in 2020, L&I transferred to Defendant the Personal  
5 Information of thousands of Washingtonians who had been injured at work and filed claims with  
6 L&I for their injuries.

7 18. Plaintiffs' Personal Information was included in this file transfer.

8 19. Defendant failed to provide reasonable security protocols necessary to safeguard  
9 this information – the security protocols were unreasonably inadequate.

10 20. On May 22, 2021, the Defendant's lax security protocols resulted in a severe data  
11 breach (the "Data Breach") by an unknown third party.

12 21. Defendant failed to timely take steps to secure the return of the Personal  
13 Information, failed to timely notify L&I of the existence of the Data Breach, failed to notify the  
14 victims of the data breach, and failed to notify local, state, and federal authorities that the crime  
15 had occurred.

16 22. Finally, on June 4, 2021, the Defendant notified L&I of the Data Breach, and L&I  
17 belatedly notified the victims several weeks later on June 29, 2021.

18 23. Defendant was aware, or should have been aware, that its systems were vulnerable  
19 to a security breach. Defendant's failure to provide adequate security protocols jeopardized the  
20 sensitive information of thousands of Washington residents, including Plaintiffs and the Class,  
21 fell well short of Defendant's obligations, and also fell short of Plaintiffs' and other Class  
22 members' reasonable expectations for protection of their private, sensitive information.

23 24. As a result of Defendant's conduct and the ensuing Data Breach, Plaintiffs and the  
24 Class members have suffered actual damages, and are at imminent risk of future harm, including  
25 identity theft and fraud that would result in monetary loss. Accordingly, Plaintiffs bring suit, on  
26

1 behalf of themselves and Class of all others similarly situated, to seek redress for Defendant's  
2 unlawful conduct.

3 **The Effect of the Data Breach on the Class**

4 25. Given the sensitive nature of the Personal Information subject to the Data Breach,  
5 hackers have the ability to commit identity theft, financial fraud, and other identity-related fraud  
6 against Plaintiffs and Class members now and into the indefinite future.

7 26. As a result of the Data Breach, Plaintiffs and Class members are forced to take a  
8 variety of steps to monitor for and safeguard against identity theft, and they are at a much greater  
9 risk of suffering such identity theft.

10 27. In addition, these victims of the Data Breach are at a heightened risk of potentially  
11 devastating financial identity theft. As the Bureau of Justice Statistics reports, identity theft causes  
12 its victims out-of-pocket monetary losses and costs the nation's economy billions of dollars every  
13 year.<sup>1</sup>

14 28. In fact, many victims of the Data Breach may have already experienced harms as  
15 a result of the Data Breach, including, but not limited to, identity theft, financial fraud, tax fraud,  
16 unauthorized lines of credit opened in their names, medical and healthcare fraud, and  
17 unauthorized access to their bank accounts. Plaintiffs and Class members have spent and will  
18 spend time, money, and effort dealing with the fallout of the Data Breach, including purchasing  
19 credit protection services, contacting their financial institutions, checking credit reports, and  
20 spending time and effort searching for unauthorized activity.

21 29. The Personal Information exposed in the Data Breach is highly coveted and  
22 valuable on underground or black markets. For example, a cyber "black market" exists in which  
23 criminals openly post and sell stolen consumer information on underground internet websites  
24 known as the "dark web"—exposing consumers to identity theft and fraud for years to come.

25  
26  

---

<sup>1</sup> See U.S. Dept. of Justice, Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013),  
available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Jul. 2, 2021).

1           30. Identity thieves can use the Personal Information to: (a) create fake credit cards  
2 that can be swiped and used to make purchases as if they were the real credit cards; (b) reproduce  
3 stolen debit cards and use them to withdraw cash from ATMs; (c) commit immigration fraud; (d)  
4 obtain a fraudulent driver's license or ID card in the victim's name; (e) obtain fraudulent  
5 government benefits; (f) file a fraudulent tax return using the victim's information; (g) commit  
6 medical and healthcare-related fraud; (h) access financial accounts and records; or (i) commit any  
7 number of other frauds, such as obtaining a job, procuring housing, or giving false information to  
8 police during an arrest.

9           31. Consumers are injured every time their data is stolen and placed on the dark web—  
10 even if they have been victims of previous data breaches.

11           32. Not only is the likelihood of identity theft increased, but the dark web is not like  
12 Google or eBay. It is comprised of multiple and discrete repositories of stolen information.

13           33. Each data breach puts victims at risk of having their information uploaded to  
14 different dark web databases and viewed and used by different criminal actors.

15           34. Exposure of this information to the wrong people can have serious consequences.

16           35. Identity theft can have ripple effects, which can adversely affect the future  
17 financial trajectories of victims' lives. For example, the Identity Theft Resource Center reports  
18 that respondents to their surveys in 2013–2016 described that the identity theft they experienced  
19 affected their ability to get credit cards and obtain loans, such as student loans or mortgages.<sup>2</sup>

20           36. For some victims, this could mean the difference between going to college or not,  
21 becoming a homeowner or not, or having to take out a high interest payday loan versus a lower-  
22 interest loan.

23           37. Annual monetary losses from identity theft are in the billions of dollars. According  
24 to a Presidential Report on identity theft produced in 2007:

25  
26  

---

<sup>2</sup> Identity Theft Resource Center, *The Aftermath 2017*, [https://www.idtheftcenter.org/images/page-docs/Aftermath\\_2017.pdf](https://www.idtheftcenter.org/images/page-docs/Aftermath_2017.pdf) (last visited Jul. 2, 2021).

1 In addition to the losses that result when identity thieves  
2 fraudulently open accounts ... individual victims often suffer  
3 indirect financial costs, including the costs incurred in both civil  
4 litigation initiated by creditors and in overcoming the many  
5 obstacles they face in obtaining or retaining credit. Victims of non-  
6 financial identity theft, for example, health-related or criminal  
7 record fraud, face other types of harm and frustration.

8 In addition to out-of-pocket expenses that can reach thousands of  
9 dollars for the victims of new account identity theft, and the  
10 emotional toll identity theft can take, some victims have to spend  
11 what can be a considerable amount of time to repair the damage  
12 caused by the identity thieves. Victims of new account identity theft,  
13 for example, must correct fraudulent information in their credit  
14 reports and monitor their reports for future inaccuracies, close  
15 existing bank accounts and open new ones, and dispute charges with  
16 individual creditors.<sup>3</sup>

17 38. As the result of the Data Breach, Plaintiffs and Class members are likely to suffer  
18 economic loss and other actual harm for which they are entitled to damages, including, but not  
19 limited to, the following:

20 (a) losing the inherent value of their Personal Information;

21 (b) costs associated with the detection and prevention of identity  
22 theft and unauthorized use of their financial accounts;

23 (c) costs associated with purchasing credit monitoring, credit  
24 freezes, and identity theft protection services;

25 (d) lowered credit scores resulting from credit inquiries following  
26 fraudulent activities;

(e) costs associated with time spent and the loss of productivity or  
the enjoyment of one's life from taking time to address and attempt  
to mitigate and address the actual and future consequences of the  
Data Breach, including discovering fraudulent charges, cancelling  
and reissuing cards, purchasing credit monitoring and identity theft  
protection services, imposing withdrawal and purchase limits on  
compromised accounts, and the stress, nuisance and annoyance of  
dealing with the repercussions of the Data Breach; and

---

<sup>3</sup> FTC, *Combating Identity Theft A Strategic Plan* (April 2007), available at <https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategicplan/strategicplan.pdf> (last visited Jul. 2, 2021).

1 (f) the continued imminent and certainly impending injury flowing  
2 from potential fraud and identify theft posed by their Personal  
3 Information being in the possession of one or many unauthorized  
4 third parties.

5 39. Even in instances where a consumer is reimbursed for a financial loss due to  
6 identity theft or fraud, that does not make that individual whole again, as there is typically  
7 significant time and effort associated with seeking reimbursement that is not refunded.

8 40. The Department of Justice's Bureau of Justice Statistics found that identity theft  
9 victims "reported spending an average of about 7 hours clearing up the issues" relating to identity  
10 theft or fraud.<sup>4</sup>

11 41. There may also be a significant time lag between when Personal Information is  
12 stolen and when it is actually misused. According to the GAO, which conducted a study regarding  
13 data breaches:

14 [L]aw enforcement officials told us that in some cases, stolen data  
15 may be held for up to a year or more before being used to commit  
16 identity theft. Further, once stolen data have been sold or posted on  
17 the Web, fraudulent use of that information may continue for years.  
18 As a result, studies that attempt to measure the harm resulting from  
19 data breaches cannot necessarily rule out all future harm.<sup>5</sup>

### 20 Plaintiffs' Individual Allegations

21 42. Each Plaintiff applied for L&I benefits from the State of Washington. As part of  
22 their applications, Plaintiffs were required to provide L&I their Personal Information.

23 43. Given the highly sensitive nature of the information stolen in the Data Breach,  
24 Plaintiffs remain at a substantial and imminent risk of future harm, including identity theft and  
25 theft from their bank accounts.

26 <sup>4</sup> E. Harrell, U.S. Department of Justice, *Victims of Identity Theft, 2014* (revised Nov. 13, 2017),  
<http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last visited Jul. 2, 2021).

<sup>5</sup> U.S. Government Accountability Office Report to Congressional Requesters, *Data Breaches Are  
Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007),  
<https://www.gao.gov/assets/gao-07-737.pdf> (last visited Jul. 2, 2021).



1 44. Plaintiffs have expended and will be required to expend additional time and effort  
2 monitoring their financial accounts and credit reports.

3 V. CLASS ACTION ALLEGATIONS

4 45. Paragraphs 1 – 44 are incorporated herein by reference.

5 46. Plaintiffs bring this action individually and on behalf of a class (the “Class”)  
6 preliminarily defined as:

7 All individuals residing in the United States whose personal  
8 information was compromised in the data breach disclosed by the  
Washington Department of Labor & Industries in July 2021.

9 Excluded from the Class are the Defendant; any agent, affiliate,  
10 parent, or subsidiary of the Defendant; any entity in which the  
11 Defendant has a controlling interest; any officer or director of the  
12 Defendant; any successor or assign of the Defendant; and any Judge  
to whom this case is assigned as well as his or her staff and  
immediate family.

13 47. Plaintiffs reserve the right to amend the class definition.

14 48. This action satisfies the numerosity, commonality, typicality, and adequacy  
15 requirements of CR 23.

16 (a) **Numerosity**. Plaintiffs are representatives of the proposed Class reportedly  
17 consisting of approximately 16,466 members—far too many to join in a single action.

18 (b) **Ascertainability**. Class members are readily identifiable from information in  
19 Defendant’s possession, custody, or control.

20 (c) **Typicality**. Plaintiffs’ claims are typical of Class members’ claims as each  
21 arises from the same Data Breach, the same alleged negligence of and/or statutory  
22 violations by Defendant, and the same unreasonable manner of notifying individuals  
23 regarding the Data Breach.

24 (d) **Adequacy**. Plaintiffs will fairly and adequately protect the interests of the  
25 proposed Class. Their interests do not conflict with Class members’ interests and they  
26 have retained counsel experienced in complex class action litigation and data privacy to

1 vigorously prosecute this action on behalf of the Class, including in the capacity as lead  
2 counsel.

3 (e) Commonality. Plaintiffs' and Class members' claims raise predominantly  
4 common factual and legal questions that can be answered for all Class members through  
5 a single class-wide proceeding. For example, to resolve any Class member's claims, it will  
6 be necessary to answer the following questions:

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

10 B. Whether Defendant's conduct was negligent;

11 C. Whether Plaintiffs and the Class are entitled to damages, treble damages, and/or  
12 injunctive relief.

13 49. In addition to satisfying the prerequisites of CR 23(a), Plaintiffs satisfy the  
14 requirements for maintaining a class action under CR 23(b). Common questions of law and fact  
15 predominate over any questions affecting only individual members, and a class action is superior  
16 to individual litigation or any other available methods for the fair and efficient adjudication of the  
17 controversy. The damages available to individual plaintiffs are insufficient to make litigation  
18 addressing Defendant's privacy practices economically feasible in the absence of the class action  
19 procedure.

20 50. In the alternative, class certification is appropriate because Defendant has acted or  
21 refused to act on grounds generally applicable to the Class, thereby making final injunctive relief  
22 appropriate with respect to the members of the Class as a whole.

23 **VI. FIRST CLAIM FOR RELIEF**  
24 **Negligence**  
*On Behalf of Plaintiffs and the Class*

25 51. Paragraphs 1 – 50 are incorporated herein by reference.  
26

1           52. Defendant negligently maintained Plaintiffs' Personal Information in an  
2 environment vulnerable to a security breach.

3           53. Defendant failed to inform L&I or the Plaintiffs that its systems were inadequate  
4 to safeguard sensitive information and that transferring Personal Information could lead to  
5 attackers gaining access to sensitive information.

6           54. Defendant did so despite advertising that it was capable of securing sensitive,  
7 confidential information.

8           55. It was reasonably foreseeable to Defendant that its failure to implement and  
9 maintain reasonable security procedures and practices appropriate to the nature and scope of use  
10 of the sensitive information to which it was entrusted could subject customers to a breach of the  
11 sensitive information, and could thus expose the owners of that information to harm.

12           56. Furthermore, given the known risk of major data breaches, Plaintiffs and the Class  
13 members are part of a well-defined, foreseeable, finite, and discernible group that was at high risk  
14 of having their Personal Information stolen.

15           57. Defendant owed a duty to Plaintiffs and members the Class to ensure that its  
16 systems and networks—and the personnel responsible for them—adequately protected their  
17 Personal Information.

18           58. Defendant's duty of care arose as a result of Defendant's knowledge that it was  
19 entrusted with, and obligated to protect, confidential and sensitive data.

20           59. Only Defendant was in a position to ensure that its systems were sufficient to  
21 protect against the harm to Plaintiffs and the members of the Class from a data breach.

22           60. In addition, Defendant had a duty to use reasonable security measures under  
23 Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair ...  
24 practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair  
25 practice of failing to use reasonable measures to protect confidential data.  
26

1           61. Defendant also had a duty to use reasonable care in protecting confidential data  
2 because it committed to complying to the highest standards for the protection of Personal  
3 Information.

4           62. Defendant knew, or should have known, of the risks inherent in its vulnerable  
5 systems and the inadequacy of its own security protocols.

6           63. By failing to use reasonable measures to secure sensitive data, by continuing to  
7 store sensitive data despite the vulnerabilities of its systems, and by failing to cure those  
8 vulnerabilities, Defendant breached its duties to Plaintiffs and the Class.

9           64. Plaintiffs and Class members have suffered harm as a result of Defendant's  
10 negligence. These victims suffered diminished value of their sensitive information.

11           65. Plaintiffs and Class members also lost control over the Personal Information,  
12 which subjected each of them to a greatly enhanced risk of identity theft, medical identity theft,  
13 credit and bank fraud, Social Security fraud, tax fraud, and myriad other types of fraud and theft,  
14 in addition to the time and expenses spent mitigating those injuries and preventing further injury.

15                                   **VII. SECOND CLAIM FOR RELIEF**  
16                   **Violation of the Washington Consumer Protection Act, RCW § 19.86, et seq.**  
17                                   ***On Behalf of Plaintiffs and the Class***

17           66. Paragraphs 1 – 65 are incorporated herein by reference.

18           67. Defendant is a “person” within the meaning of the Washington Consumer  
19 Protection Act, RCW 19.86.010(1), and it conducts “trade” and “commerce” within the meaning  
20 of RCW 19.86.010(2).

21           68. Plaintiffs and other members of the Class are “persons” within the meaning of  
22 RCW 19.86.010(1).

23           69. Defendant's failure to safeguard the Personal Information exposed in the Data  
24 Breach constitutes an unfair act that offends public policy.

25           70. Defendant's failure to safeguard the Personal Information compromised in the  
26 Data Breach caused substantial injury to Plaintiffs and Class members.

1           71. Defendant's failure is not outweighed by any countervailing benefits to consumers  
2 or competitors, and it was not reasonably avoidable by consumers.

3           72. Defendant's failure to safeguard the Personal Information disclosed in the Data  
4 Breach, and its failure to provide timely and complete notice of that Data Breach to the victims,  
5 is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

6           73. Defendant's unfair acts or practices occurred in its trade or business and have  
7 injured and are capable of injuring a substantial portion of the public.

8           74. Defendant's general course of conduct as alleged herein is injurious to the public  
9 interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of  
10 being repeated.

11           75. As a direct and proximate result of Defendant's unfair acts or practices, Plaintiffs  
12 and Class members suffered injury in fact.

13           76. As a result of Defendant's conduct, Plaintiffs and members of the Class have  
14 suffered actual damages, including the lost value of their Personal Information; the lost value of  
15 their personal data and lost property in the form of their breached and compromised Personal  
16 Information (which is of great value to third parties); ongoing, imminent, and certainly impending  
17 threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm;  
18 loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data  
19 on the dark web black market; expenses and/or time spent on credit monitoring and identity theft  
20 insurance; time spent scrutinizing bank statements, credit card statements, and credit reports;  
21 expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work  
22 time; and other economic and non-economic harm.

23           77. Plaintiffs and Class members are entitled to an order enjoining the conduct  
24 complained of herein and ordering Defendant to take remedial measures to prevent similar data  
25 breaches; actual damages; treble damages pursuant to RCW § 19.86.090; costs of suit, including  
26 reasonable attorney's fees; and such further relief as the Court may deem just and proper.

VIII. PRAYER FOR RELIEF

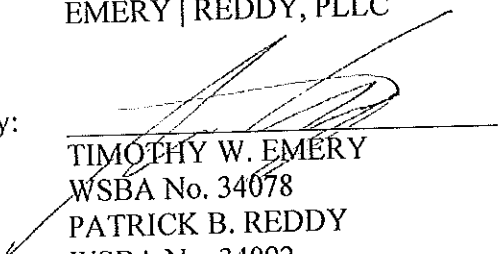
Plaintiffs request that the Court enter judgment against Defendant as follows:

- A. Certifying the proposed Class pursuant to Civil Rule 23 and appointing Plaintiffs and their counsel to represent the Class;
- B. Awarding Plaintiffs and Class members monetary relief, including actual and treble damages and penalties;
- C. Ordering equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein and compelling Defendant to utilize appropriate methods and policies with respect to maintaining the security of the sensitive and confidential information in its possession belonging to Washington citizens.
- D. Awarding costs of suit and attorney's fees, as permitted by law;
- E. Awarding of pre-judgment and post-judgment interest, as permitted by law;
- and
- F. Such other and further relief as this Court may deem just and proper.

DATED this 2<sup>nd</sup> day of July 2021.

EMERY | REDDY, PLLC

By:

  
 TIMOTHY W. EMERY  
 WSBA No. 34078  
 PATRICK B. REDDY  
 WSBA No. 34092  
 Emery Reddy, PLLC  
 600 Stewart Street, Suite 1100  
 Seattle, WA 98101  
 Telephone: (206) 442-9106  
 Fax: (206) 441-9711  
 Email: emeryt@emeryreddy.com  
 Email: reddyp@emeryreddy.com  
*Attorneys for Plaintiffs Gary Steve Clopp,  
 Shlon Smithson, and LeeAnn Crawford*

# EXHIBIT 1

Out of an abundance of caution, L&I and PMR are notifying the workers by mail and offering 12 months of free credit monitoring.

Although L&I account numbers for employers are public information, L&I is also notifying the workers' 9,400 employers whose L&I account numbers were also included in the document. Both mailings should start arriving today.

###

**For media information:**

**Rich Roesler** (<mailto:Rich.Roesler@Lni.wa.gov>), L&I Public Affairs, **360-628-3034**

**Connect with L&I:**

**Facebook** (<https://www.facebook.com/laborandindustries>) ([www.facebook.com/laborandindustries](http://www.facebook.com/laborandindustries))

**Twitter** (<https://www.twitter.com/lniwa>) ([www.twitter.com/lniwa](http://www.twitter.com/lniwa))

---

Communication Services | [www.Lni.wa.gov/news-events](http://www.Lni.wa.gov/news-events) (<https://lni.wa.gov/news-events>) | **360-902-5400** (<tel:3609025400>)

[See the latest L&I news releases](https://lni.wa.gov/news-events) (<https://lni.wa.gov/news-events>)



**SUBSCRIBE TO NEWS RELEASES**

([HTTPS://PUBLIC.GOVDELIVERY.COM/ACCOUNTS/WADLI/SUBSCRIBER/NEW](https://PUBLIC.GOVDELIVERY.COM/ACCOUNTS/WADLI/SUBSCRIBER/NEW))