JASON R. HULL [11202]
JHULL@MOHTRIAL.COM
TREVOR C. LANG [14232]
TLANG@MOHTRIAL.COM
MARSHALL OLSON & HULL, PC
NEWHOUSE BUILDING
TEN EXCHANGE PLACE, SUITE 350
SALT LAKE CITY, UTAH 84111
TELEPHONE: 801.456.7655

ATTORNEYS FOR PLAINTIFF AND
PROPOSED CLASS COUNSEL

RAINA C. BORRELLI*
RAINA@TURKESTRAUSS.COM
SAMUEL J. STRAUSS*
SAM@TURKESTRAUSS.COM
ALEX PHILLIPS*
ALEXP@TURKESTRAUSS.COM
TURKE & STRAUSS, LLP
613 WILLIAMSON STREET, SUITE 201
MADISON, WI 53703
TELEPHONE: 608.237.1775
*PRO HAC VICE FORTHCOMING

IN THE UNITED STATES DISTRICT COURT
DISTRICT OF UTAH, CENTRAL DIVISION

JIM VANSICKLE, an individual on behalf of himself and all others similarly situated, Plaintiff, v. C.R. ENGLAND, INC., a Utah Corporation, Defendant.	**COMPLAINT** **[PROPOSED CLASS ACTION]** **JURY TRIAL DEMANDED** Case No.: 2:22-cv-374-DBP

Plaintiff, Jim Vansickle ("Plaintiff") brings this action on behalf of himself, and all others similarly situated against Defendant, C.R. England, Inc., ("C.R. England" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

NATURE OF THE ACTION

1. On or about October 30, 2021, C.R. England, a national refrigerated carrier and trucker training school, discovered that it lost control over at least 224,572 former and current

students' and employees' highly sensitive personal records in a data breach by cybercriminals ("Data Breach").

2. On information and belief, it is unclear how long the Data Breach carried on undetected.

3. On April 20, 2022—nearly six months after discovering the Data Breach—C.R. England's investigations revealed that hackers gained unauthorized access to students' and employees' confidential personal identifying information ("PII").

4. Upon information and belief, the stolen PII included, at least, students' and employees' names and Social Security numbers.

5. After C.R. England's "investigation" inexplicably dragged on for nearly six months, C.R. England finally disclosed the Data Breach to its students and employees on or around May 23, 2022 (the "Breach Notice").

6. When C.R. England finally announced the Data Breach, it deliberately underplayed the breach's severity and misrepresented that "[it had] no reason to believe that [the compromised] information was published, shared, or misused as a result of [the] incident," even though C.R. England knew cybercriminals had infiltrated its systems. A true and correct copy of the Breach Notice is attached hereto as Exhibit A.[1]

7. C.R. England's failure to timely detect and report the Data Breach made its students and employees vulnerable to identify theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

[1] Breach Notice obtained from the website of the office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/b9c7cbd5-3a6f-4132-a6b5-b6dd3ee1eef3.shtml (last visited June 2, 2022).

8. C.R. England's failure to protect students' and employees' PII and adequately warn them about the Data Breach violates Utah and California law, harming thousands of current and former C.R. England students and employees.

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

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

11. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

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

THE PARTIES

13. Plaintiff, Jim Vansickle, is an adult resident and citizen of California. Mr. Vansickle intends to remain domiciled in California indefinitely, and maintains his true, fixed, and permanent home in California. Mr. Vansickle is a former C.R. England student and employee and his PII was compromised by the Data Breach.

14. Defendant C.R. England is a Utah corporation with its principal place of business located at 4701 W. 2100 South, Salt Lake City, UT 84120.

15. Defendant C.R. England has other truck driving school locations in Colton, California; Laredo, Texas; and Valparaiso, Indiana.

JURISDICTION & VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action in which the amount in controversy exceeds $5 million, exclusive of costs and interest, there are more than 100 members in the proposed class, and at least one class member is a citizen of a different state than C.R. England, establishing minimal diversity.

17. This Court has personal jurisdiction over C.R. England because it is incorporated in Utah and its corporate headquarters is in Salt Lake City, Utah.

18. Venue is proper in this Court under 28 U.S.C. §§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because C.R. England conducts business in this District.

COMMON FACTUAL ALLEGATIONS

C.R. England's Failure to Prevent the Data Breach

19. Plaintiff and members of the proposed Class are C.R. England's current and former students and employees.

20. To enroll in C.R. England's truck driving schools, and to obtain employment, C.R. England requires its students and employees to provide their PII.

21. C.R. England maintains records of its students' and employees' information, including their full names and Social Security Numbers. These records are stored on C.R. England's computer systems.

22. When C.R. England collects this sensitive information, it promises to use reasonable measures to safeguard the PII from theft and misuse.

23. In fact, C.R. England informs its employees that it collects and maintains their PII through the Privacy Policy (the "Privacy Policy").[2] A true and correct copy of the Privacy Policy is attached hereto as Exhibit B.

24. The Privacy Policy warrants that C.R. England "recognizes the importance of protecting information and data [it] collects." Exh. B.

25. The Privacy Policy also highlights C.R. England's promise to "safeguard the information and data [potential employees] provide to [C.R. England] from unauthorized access and unauthorized disclosure . . ." *Id.*

[2] *See* C.R. England's Website: https://www.crengland.com/about-us/privacy-policy (last visited June 2, 2022).

26. C.R. England represented to its students, employees, and prospective employees that their PII would be secure. Plaintiff and members of the proposed Class relied on such representations when they agreed to provide their PII to C.R. England.

27. Despite its alleged commitments to securing sensitive employee data, C.R. England does not follow industry standard practices in securing employees' PII.

28. In October 2021, hackers bypassed C.R. England's security safeguards and infiltrated its systems, giving them access to student and employee PII.

29. In response to the Data Breach, C.R. England contends that it has "implemented security measures to protect [its] digital environment and minimize the likelihood of future incidents." Exh. A. These measures should have been in place *before* the Data Breach.

30. C.R. England's Breach Notice omits the size and scope of the breach. C.R. England has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

31. On information and belief, the Data Breach has impacted at least 224,572 C.R. England students and employees.

32. On information and belief, C.R. England does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

33. C.R. England's negligent conduct caused the Data Breach. C.R. England violated its obligation to implement best practices and comply with industry standards concerning computer system security. C.R. England failed to comply with security standards and allowed its students' and employees' PII to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

34. C.R. England ultimately admitted to the Data Breach on or about May 23, 2022—nearly seven months after discovering the breach. C.R. England has failed to justify the delays in notifying breach victims.

35. C.R. England encouraged Data Breach victims to "remain vigilant by reviewing [their] account statements and credit reports closely." Exh. A.

36. On information and belief, C.R. England has offered breach victims only one year of complimentary identity theft protection services through IDX.

37. As more fully articulated below, Plaintiff's and the members of the proposed Class's personal data may exist on the dark web and in the public domain for months, or even years, before it is used for ill gains and actions. With only one year of monitoring, and no form of insurance or other protection, Plaintiff and members of the proposed Class remain unprotected from the real and long-term threats against their personal, sensitive, and private data.

38. Therefore, the "protection" services offered by C.R. England are inadequate, and Plaintiff and the members of the proposed Class have a real and cognizable interest in obtaining equitable relief, in addition to the monetary relief requested herein.

Plaintiff's Experience

39. Plaintiff Jim Vansickle is a former C.R. England student and employee.

40. As a condition of receiving C.R. England's services, training, and employment, C.R. England required Plaintiff to provide his PII, and Plaintiff indeed provided C.R. England with his PII to C.R. England.

41. In late May 2022, Plaintiff received a notice letter from C.R. England confirming his PII was compromised as a result of the Data Breach.

42. Plaintiff has spent, and will have to spend, considerable time and effort over the coming years monitoring his accounts to protect himself from identity theft. Plaintiff's personal financial security has been jeopardized and there is uncertainty over what personal information was revealed in the Data Breach.

43. Further, Plaintiff is unsure what has happened to his PII as C.R. England has been unwilling to disclose the true nature of the Data Breach.

44. Had Plaintiff known that C.R. England does not adequately protect PII, he would not have transacted with C.R. England. Furthermore, Plaintiff's sensitive PII remains in C.R. England's possession without adequate protection against known threats, exposing Plaintiff to the prospect of additional harm in the event C.R. England suffers another data breach.

Plaintiff and the Class Face Significant Risk of Identity Theft

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

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

47. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[3]

[3] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/ (last visited June 2, 2022).

48. As a result of Defendant's failure to prevent, and timely report the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses and lost time. They have also suffered or are at an increased risk of suffering:

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

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

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

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

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

49. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained. [4]

[4] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 2, 2022).

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

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

52. One such example of criminals using PII for profit is the development of "Fullz" packages. [5]

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

54. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII

[5] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), *available at* https://krebsonsecurity.com/tag/fullz/ (last visited June 2, 2022).

stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

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

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

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

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

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

60. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[6]

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

---

[6] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited June 2, 2022).

[7] *Start With Security, A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited June 2, 2022).

[8] *Id.*

62. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history, and reputation, and can take time, money, and patience to resolve the fallout. [9] The FTC treats 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(a) of the FTC Act.

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

[9] *See* Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited Jan. 18, 2022).

all preceded the Data Breach, further clarify the measures businesses must take to meet their data security obligations.

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

65. Defendant's failure to properly and promptly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps in an effort to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

66. **Definition of the Class.** Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 and DUCivR 23-1(b) on behalf of himself and all members of the proposed classes (together the "Class"), defined as follows:

> **Nationwide Class:** All individuals residing in the United States whose personal information was compromised in the Data Breach disclosed by C.R. England in May 2022.
>
> **California Subclass:** All individuals residing in California whose personal information was compromised in the Data Breach disclosed by C.R. England in May 2022.

67. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent

has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

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

69. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

70. Plaintiff and members of the Class satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23:

a. **Numerosity**. The exact number of the members of the Class is unknown but, upon information and belief, the number of Class members exceeds 224,500, and individual joinder in this case is impracticable. Members of the Class can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

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

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

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

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

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

iii. Whether Defendant breached its contractual promises to safeguard Plaintiff's and members of the Class's PII;

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

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

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

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

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

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

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

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

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

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

xiv. What the proper measure of damages is; and

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

e. **Superiority:** A class action is also a fair and efficient method of adjudicating the controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given

the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendant's misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured

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

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

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

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiff and the Class)

72. Plaintiff incorporates all previous paragraphs as if fully set forth below.

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

74. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who made that happen.

75. 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.

76. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable time frame of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and

occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

77. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's PII for trucker training and employment purposes. Plaintiff and members of the Class needed to provide their PII to Defendant to receive training and employment from Defendant, and Defendant retained that information.

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

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

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

81. Defendant also breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and members of the Class's injuries-in-fact.

82. As a direct and traceable result of Defendant's negligence or negligent supervision, Plaintiff, and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

SECOND CLAIM FOR RELIEF
Negligence Per Se
(On Behalf of Plaintiff and the Class)

84. Plaintiff incorporates all previous paragraphs as if fully set forth below.

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

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

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

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

89. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PII.

90. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's PII.

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

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

93. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

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

95. As a direct and proximate result of Defendant's negligence per se, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
Breach of Contract, Including the Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates all previous paragraphs as if fully set forth below.

97. Defendant offered to provide goods and services to Plaintiff and members of the Class who were trucking school students in exchange for payment.

98. Defendant also required Plaintiff and the members of the Class who were students to provide Defendant with their PII to receive services and training.

99. Defendant required the members of the Class who were employees to provide Defendant with their PII to receive services and/or as a condition of their employment.

100. In turn, Defendant agreed it would not disclose the PII it collects from employees to unauthorized persons. Defendant also impliedly promised to maintain safeguards to protect its employees' PII. Indeed, Defendant stated that it "recognizes the importance of protecting information and data [collected]" and that it has "put in place reasonable electronic and procedures to help safeguard the information and data . . . from unauthorized access and unauthorized disclosure. . ." Exh. B.

101. Class members who are employees accepted Defendant's offer of employment by providing their PII to Defendant.

102. Implicit in the parties' agreement was that Defendant would provide Plaintiff and members of the Class with prompt and adequate notice of all unauthorized access or theft of their PII.

103. Plaintiff and the members of the Class would not have entrusted their PII to Defendant without such agreement with Defendant.

104. Defendant materially breached the contracts it had entered with Plaintiff 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 also breached the implied contracts with Plaintiff and members of the Class by:

a. Failing to properly safeguard and protect Plaintiff's and members of the Class's PII;

b. Violating industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

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

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

106. Plaintiff and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

107. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on 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 along with its form.

108. 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.

109. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

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

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

112. Plaintiff, on behalf of himself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of the Plaintiff and the Class)

113. Plaintiff incorporates all previous paragraphs as if fully set forth below.

114. This claim is plead in the alternative to the Third Claim for Relief.

115. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of monies paid for trucker training services and through employment.

116. Defendant appreciated or knew about the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff's and members of the Class's PII, as this was used to facilitate employment processing, payroll, and trucker training services.

117. As a result of Defendant's conduct, Plaintiff and members of the Class who are former or current trucking students suffered actual damages in an amount equal to the difference in value between their training cost payments made with reasonable data privacy and security practices and procedures that Plaintiff and members of the Class paid for, and those training cost

payments made without unreasonable data privacy and security practices and procedures that they received.

118. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's payments and their PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII, nor used and paid for Defendant's goods and services had they known Defendant would fail to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiff and members of the Class paid for and that were otherwise mandated by federal, state, and local laws, and industry standards.

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

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of the Plaintiff and the Class)

120. Plaintiff incorporates all previous paragraphs as if fully set forth below.

121. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

122. Defendant owed a duty to its students and employees, including Plaintiff and the Class, to keep this information confidential.

123. The unauthorized acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

124. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant to receive trucking training services and employment, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

125. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

126. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

127. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

128. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

129. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

130. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

131. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

132. In addition to injunctive relief, Plaintiff, on behalf of himself and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

SIXTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150
(On Behalf of the Plaintiff and the California Subclass)

133. Plaintiff incorporates all previous paragraphs as if fully set forth below.

134. Defendant violated § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted PII of Plaintiff. As a direct and proximate result, Plaintiff's PII was subject to unauthorized access and exfiltration, theft, or disclosure.

135. Defendant is a business organized for the profit and financial benefit of its owners according to § 1798.140, with annual gross revenues exceeding the threshold established by § 1798.140(c).

136. Plaintiff seeks injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold PII, including Plaintiff's PII. Plaintiff has an interest in ensuring that his PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

137. Pursuant to Cal. Civ. Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

138. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the personal information under the CCPA.

139. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

SEVENTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. Code § 17200, *et seq.*
(On behalf of Plaintiff and the California Subclass)

140. Plaintiff incorporates all previous paragraphs as if fully set forth below.

141. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

142. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

143. Defendant stored the PII of Plaintiff and the California Subclass in its computer systems and knew or should have known it did not employ reasonable, industry standard, and

appropriate security measures that complied with applicable regulations and that would have kept Plaintiff and the California Subclass's PII secure and prevented the loss or misuse of that PII.

144. Defendant failed to disclose to Plaintiff and the California Subclass that their PII was not secure. However, Plaintiff and the California Subclass were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff and the California Subclass on notice that their PII was not secure, which Defendant had a duty to disclose.

145. Defendant also violated California Civil Code § 1798.150 by failing to employ reasonable security measures, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the California Subclass's PII.

146. Had Defendant complied with these requirements, Plaintiff and the California Subclass would not have suffered the damages related to the data breach.

147. Defendant's conduct was unlawful, in that it violated the Consumer Records Act.

148. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

149. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

150. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of

computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

151. Instead, Defendant made the PII of Plaintiff and the California Subclass accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the California Subclass to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

152. As a result of those unlawful and unfair business practices, Plaintiff and the California Subclass suffered an injury-in-fact and have lost money or property.

153. The injuries to Plaintiff and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

154. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

155. Therefore, Plaintiff and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

EIGHTH CLAIM FOR RELIEF
Declaratory Judgment and Injunctive Relief
(On behalf of Plaintiff and the Class)

156. Plaintiff incorporates all previous paragraphs as if fully set forth below.

157. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious and which violate the terms of the federal and state statutes described above.

158. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiff alleges Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiff and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

159. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed, and continues to owe, a legal duty to employ reasonable data security to secure the PII with which it is entrusted from its employees and students, and to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

b. Defendant breached, and continues to breach, its duty by failing to employ reasonable measures to secure its employees' and students' personal information; and

c. Defendant's breach of its legal duty continues to cause harm to Plaintiff and the Class.

160. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its current and former employees' and students' (*i.e.*, Plaintiff's and the Class's) data.

161. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

162. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

163. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiff, the Class, and the public at large.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, demands 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 Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

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

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

D. Enjoining C.R. England from further deceptive and unfair practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include compensatory, exemplary, punitive damages, and statutory damages, including pre- and post-judgment interest, in an amount to be proven at trial;

F. Awarding restitution and damages to Plaintiff 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 Plaintiff 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.

JURY DEMAND

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

DATED this 3rd day of June, 2022.

MARSHALL OLSON & HULL, PC

BY: /s/ Trevor C. Lang
JASON R. HULL
TREVOR C. LANG

TURKE & STRAUSS, LLP
RAINA C. BORRELLI
SAMUEL J. STRAUSS
ALEX PHILLIPS

ATTORNEYS FOR PLAINTIFF AND
PROPOSED CLASS COUNSEL

C.R.England
Return to IDX
P.O Box 989728
West Sacramento, CA 95798-9728

TO ENROLL, PLEASE CALL:
1-833-909-0993
OR VISIT:
https://response.idx.us/cr-england
Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

May 23, 2022

RE: Notice of Data <<Variable Field 1>>.

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a recent data security incident experienced by C.R. England that may have involved your personal information. Please read this letter carefully as it contains information regarding the incident, the type of information potentially involved, and the steps that you can take to help protect your personal information.

What Happened: On October 30, 2021, we discovered unauthorized activity on our systems. In response, we immediately began containment, mitigation, and restoration efforts to terminate the activity and to secure our network, systems, and data. In addition, we retained independent cybersecurity experts to conduct a forensic investigation into the incident and assist us in determining what happened.

The forensic investigation determined that there was unauthorized access to certain files stored within our systems. Based on these findings, we reviewed the affected files to identify the individuals whose personal information may have been impacted by this incident and the categories of information involved for each individual. On April 20, 2022, we determined that the affected files contained some of your personal information. We then worked diligently to identify current address information necessary to notify you of the incident. Please note that to date**, we have no reason to believe that your information was published, shared, or misused** as a result of this incident. Nevertheless, we are notifying you of the incident and providing resources to help protect your information.

What Information Was Involved: The information involved included the following data elements: your <<Variable Field 3>>.

What We Are Doing: After the steps described above, we implemented additional security measures to protect our digital environment and minimize the likelihood of future incidents. We also reported the incident to the Federal Bureau of Investigation and will cooperate to help identify and prosecute those responsible.

In addition, we are offering you <<12 or 24>> months of complimentary identity theft protection services through IDX, a data breach and identity recovery services expert. The identity protection services include credit monitoring, dark web monitoring, $1 million identity theft reimbursement insurance, and fully managed identity recovery services at no cost to you. To receive these services, you must be over the age of 18 and have a Social Security number, an established credit file, and a residential address in the United States that is associated with your credit file.

What You Can Do: You can enroll in the complimentary identity protection services offered in this letter by calling 1-833-909-0993 or visiting https://response.idx.us/cr-england and using the Enrollment Code provided at the top of this letter. Please note that the deadline to enroll is August 23, 2022. You can also review the enclosed sheet that provides additional steps you can take to help protect your information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered, please call 1-833-909-0993, Monday through Friday from 7:00 a.m. to 7:00 p.m. Mountain Time.

The privacy and security of your information is a top priority for C.R. England. We take this incident very seriously and we regret any worry or inconvenience this may cause you.

Sincerely,

Chad England, Chief Executive Officer
C.R. England

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
www.consumer.ftc.gov and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet & Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
www.ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
www.oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf.

Privacy Policy

Application and Consent

This Privacy Policy, effective 12/22/20 discloses the privacy policy and practices for C.R. England, Inc., a Utah corporation ("C.R. England"), and to the information and data collected through our websites at crengland.com or drivecre.com (collectively "the Site"), over the telephone, or in p Use of the words "we" and "our" refer to C.R. England. Use of the words "you" and "your" refer to you. This Privacy Policy applies to our online ar recruiting related practices as noted herein and not to other areas of C.R. England. By accessing and/or using the Site, and/or providing informat about yourself to us over the telephone or otherwise, you are consenting to the collection, storage, disclosure and use of that information and d described below, and to acceptance of the terms, conditions and practices, described in this Privacy Policy. If you submit a job application or req for information online, you agree that you are expressly authorizing C.R. England, its affiliates, or third parties to contact you at any address, tel number or email address you have provided to communicate with you regarding your application for employment with C.R. England or other employment opportunities. You agree that C.R. England, its affiliates, or third parties engaged by C.R. England may use SMS (text) messages, aut telephone dialing systems or pre-recorded messages in connection with calls made to any telephone number you have entered, even if the telep number is assigned to a cellular telephone service or other service for which the called party is charged. You understand that C.R. England may r telephone conversations you have with its representatives for quality control and training purposes and you consent to the recording of those c You understand that agreeing to these terms is not a requirement of applying for a job with C.R. England. You understand that you may apply in at any C.R. England terminal. You acknowledge that C.R. England is the sole owner of the aggregated information and data collected.

Commitment to Privacy and Limitations

C.R. England recognizes the importance of protecting information and data we collect from you. We have put in place reasonable electronic and procedures to help safeguard the information and data you provide to us from unauthorized access and unauthorized disclosure, subject to the and conditions of this Privacy Policy. However, no transmission, transfer or storage of information and data submitted or collected online can b completely secure.

Use of Cookies

Our Site may use "cookies" to collect, store and track information about you and how you use our Site. A cookie is a small piece of information s a web server to your web browser and stored on your hard drive so that it can later be read back from your web browser. Cookies are a feature browser software. They can simplify subsequent interactions with the Site and streamline transactions on related web pages, thus making your experience easier and more personalized. If you want to disable or modify cookies, most web browsers will allow you to do so. If you elect to dis or modify cookies, you may be unable to use certain features of the Site and other consequences may result.

Collection and Use of Information and Data

Information you voluntarily provide about yourself, including, but not limited to, your name, street address, city and/or state of residence, e-mai address, telephone number, work history and other information and data may be collected and stored by C.R. England. C.R. England does not ac any information or data provided on a confidential or proprietary basis except as required by law. C.R. England may use the information you pro on the Site or in connection with your job application in order to contact you, request further information, supply information and data to you, c other purposes. In addition, C.R. England may share the information you provide with its affiliates as well as third parties, including other transportation service providers, data cooperatives, and others. If you would prefer that the information you provide not be shared with third p

or categories of third parties, you may send an e-mail to unsubscribe@crengland.com requesting that C.R. England not share your inforr on v third parties and your request will be honored by C.R. England. When you use the Site, C.R. England does not allow third parties to collect infor about your online activities on the Site or across different websites.

Disclosure for Legal Reasons

C.R. England may also disclose information and data that you provide when it believes that the law requires such disclosures or if it has a good fa belief that such action is necessary or appropriate to comply with the law. Examples of such disclosure include, without limitation, to protect an defend the rights or property of C.R. England, to protect the personal safety of the public or the users of the Site, to comply with legal process, t enforce the terms of this Privacy Policy, and to respond to claims.

Children

We have no way of distinguishing the age of individuals who access our Site. We do not intend to collect any personal information from childrer the age of 18. If a parent or guardian of a child who has provided us with personal information would like the information deleted from our reco or she should contact us at unsubscribe@crengland.com. We will then make reasonable efforts to delete the child's personal information from files. We may also delete it in our own discretion. No person under the age of 13 should disclose information on this Site. If we become aware t personally identifiable information regarding a child under the age of 13 has been collected at the Site, we will make reasonable efforts to delet from our records or to otherwise respond as required by law.

Links to Other Websites

This Site contains links to other websites. Other websites, including those that we link to, have their own privacy and online policies. C.R. Engla no responsibility or control over the privacy, information collection, or other online practices of such parties. Links from our Site to their websit not constitute approval or an endorsement of the information, materials, data, content, or practices relating to those websites. You should loca review the privacy and online policies of each website that you visit to determine what information or data they may be collecting about you.

Review and Correction of Your Information

If you wish to review or correct inaccuracies in your personally identifiable information which you have provided to us through the Site, or othe please send an e-mail to unsubscribe@crengland.com identifying the inaccuracy and providing us with the correct information.

California Residents

The following disclosure applies to California residents pursuant to the California Consumer Privacy Act ("CCPA").

Personal Information Collected by C.R. England, Inc.

In connection with your application for employment, or subsequent employment at C.R. England, Inc. (the "Company"), the Company may collec information from the following categories about you:

· Personal Identifiers such as your name, employee ID number, home address, telephone number, email address; date of birth, SSN, marital statu residency and work permit status, veteran status, race, and nationality;

· Biometric information, such as height, weight, clothing size, smoking preferences, physical limitations, drug and alcohol testing results, DOT re medical information;

· Audio and/or visual information captured on security systems at our Company locations;

· Information connected to your use of facility key cards and corporate P-Cards (if applicable).

· Telematics and locational information collected through Company equipment;

· Employment-related information, such as wage, benefit and retirement account information, payroll, tax, and banking details, data from job interviews, work history, educational history, internal training records, results of credit and criminal background checks (where applicable and permitted by law), motor vehicle and licensing records.

Uses of Collected Information

We collect this information for the following purposes:

· To manage our employment relationship with you, including determining your eligibility for employment; administration of payroll and benefit managing and facilitating work related travel; internal development and training; auditing and compliance; performance evaluations; processing related to your employment (e.g., health benefits, worker compensation, insurance claims); employee/applicant communications, and other gen administrative related purposes;

· To comply with applicable law;

· To defend or protect company interests in legal or administrative proceedings.

Access to Collected Information by Third Parties

The Company may share information collected about you, as necessary and/or required by law, with:

· Third parties who provide services to the Company in connection with the operation of our business or the administration of employee benefit as IT service providers, claims administrators, human resources services, financial investment service providers, medical service providers, and insurance providers;

· Your banks or financial institution(s) and the Company's banks or financial institution(s);

· Governmental agencies, authorities, and law enforcement, if required by law.

· The Company's professional advisors as necessary (i.e. lawyers, accountants, auditors, and other professional advisers).

· Pursuant to a valid subpoena or other court order.

Changes and Updates to Privacy Policy

We reserve the right to change or update this Privacy Policy at any time without notice to you or others by posting new versions with new effec dates on the Site or through other means as we may determine. Your continued use of the Site indicates your agreement to the changes and up You should review the Privacy Policy each time you access the Site so that you are aware of any changes or updates.

How to Contact Us

We welcome your comments and questions regarding this Privacy Policy, the Site, or related matters. If you wish to contact us, please send us a mail at unsubscribe@crengland.com.

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
JIM VANSICKLE

(b) County of Residence of First Listed Plaintiff Butte County, California
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
MARSHALL OLSON & HULL, PC, 10 EXCHANGE Pl., Ste. 350, SLC, UT 84111, 801.456.7655

DEFENDANTS
C.R. ENGLAND, INC.

County of Residence of First Listed Defendant Salt Lake County
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Claims for negligence, breach of implied covenant, equitable, and California statutory claims regarding data breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
06/03/2022

SIGNATURE OF ATTORNEY OF RECORD
/s/Trevor C. Lang

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

ClassAction.org
