State of Alabama Unified Judicial System Form C-34 Rev. 7/2023	**SUMMONS** **- CIVIL -**	**Court Case Number** 68-CV-2025-900681.00

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
JEVON WORRELL V. ROBBIE D. WOOD, INC.

NOTICE TO: ROBBIE D. WOOD, INC., 1051 OLD WARRIOR RIVER RD, DOLOMITE, AL 35061
(Name and Address of Defendant)

THE COMPLAINT OR OTHER DOCUMENT WHICH IS ATTACHED TO THIS SUMMONS IS IMPORTANT, AND YOU MUST TAKE IMMEDIATE ACTION TO PROTECT YOUR RIGHTS. YOU OR YOUR ATTORNEY ARE REQUIRED TO FILE THE ORIGINAL OF YOUR WRITTEN ANSWER, EITHER ADMITTING OR DENYING EACH ALLEGATION IN THE COMPLAINT OR OTHER DOCUMENT, WITH THE CLERK OF THIS COURT. A COPY OF YOUR ANSWER MUST BE MAILED OR HAND DELIVERED BY YOU OR YOUR ATTORNEY TO THE PLAINTIFF(S) OR ATTORNEY(S) OF THE PLAINTIFF(S), JONATHAN S. MANN
[Name(s) of Attorney(s)]

WHOSE ADDRESS(ES) IS/ARE: 2001 PARK PLACE N., STE. 1100, BIRMINGHAM, AL 35203
[Address(es) of Plaintiff(s) or Attorney(s)]

THIS ANSWER MUST BE MAILED OR DELIVERED WITHIN 30 DAYS AFTER THIS SUMMONS AND COMPLAINT OR OTHER DOCUMENT WERE SERVED ON YOU OR A JUDGMENT BY DEFAULT MAY BE RENDERED AGAINST YOU FOR THE MONEY OR OTHER THINGS DEMANDED IN THE COMPLAINT OR OTHER DOCUMENT.

TO ANY SHERIFF OR ANY PERSON AUTHORIZED BY THE ALABAMA RULES OF CIVIL PROCEDURE TO SERVE PROCESS:

☐ You are hereby commanded to serve this Summons and a copy of the Complaint or other document in this action upon the above-named Defendant.

☑ Service by certified mail of this Summons is initiated upon the written request below of JEVON WORRELL *[Name(s)]* pursuant to the Alabama Rules of the Civil Procedure.

08/20/2025 *(Date)* /s/ KAREN DUNN BURKS *(Signature of Clerk)* By: _____ *(Name)*

☑ Certified Mail is hereby requested. /s/ JONATHAN S. MANN *(Plaintiff's/Attorney's Signature)*

RETURN ON SERVICE

Certified Mail

☐ Return receipt of certified mail received in this office on _____ *(Date)*.

Personal/Authorized

☐ I certify that I personally delivered a copy of this Summons and the Complaint or other document to _____ *(First and Last Name of Person Served)* in _____ *(Name of County)* County, Alabama on _____ *(Date)*.

Document left:

☐ with above-named Defendant;
☐ with an individual authorized to receive service of process pursuant to Rule 4(c), Alabama Rules of Civil Procedure;
☐ at the above-named Defendant's dwelling house or place or usual place of abode with some person of suitable age and discretion then residing therein.

Return of Non-Service

☐ I certify that service of process of this Summons and the Complaint or other document was refused by _____ *(First and Last Name of Person Served)* in _____ *(Name of County)* County, Alabama on _____ *(Date)* who is:

☐ the above-named Defendant;
☐ an individual authorized to receive service of process pursuant to Rule 4(c), Alabama Rules of Civil Procedure;

☐ As a designated process server pursuant to Rule 4(i)(1)(B), Alabama Rules of Civil Procedure, I certify that I am at least 19 years of age, I am not a party to this proceeding, and I am not related within the third degree by blood or marriage to the party seeking service of process.

_____ *(Type of Process Server)* _____ *(Server's Signature)* _____ *(Address of Server)*

_____ *(Badge or Precinct Number of Sheriff or Constable)* _____ *(Server's Printed Name)*

_____ *(Badge or Precinct Number of Sheriff or Constable)* _____ *(Telephone Number of Designated Process Server)*

ELECTRONICALLY FILED
8/20/2025 1:21 PM
68-CV-2025-900681.00
CIRCUIT COURT OF
JEFFERSON COUNTY, ALABAMA
KAREN DUNN BURKS, CLERK

State of Alabama
Unified Judicial System
Form ARCiv-93 Rev. 9/18

COVER SHEET
CIRCUIT COURT - CIVIL CASE
(Not For Domestic Relations Cases)

Ca: 68
Date of Filing: 08/20/2025
Judge Code:

GENERAL INFORMATION

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
JEVON WORRELL v. ROBBIE D. WOOD, INC.

First Plaintiff: ☐ Business ☑ Individual ☐ Government ☐ Other

First Defendant: ☑ Business ☐ Individual ☐ Government ☐ Other

NATURE OF SUIT: Select primary cause of action, by checking box (check only one) that best characterizes your action:

TORTS: PERSONAL INJURY
- ☐ WDEA - Wrongful Death
- ☑ TONG - Negligence: General
- ☐ TOMV - Negligence: Motor Vehicle
- ☐ TOWA - Wantonness
- ☐ TOPL - Product Liability/AEMLD
- ☐ TOMM - Malpractice-Medical
- ☐ TOLM - Malpractice-Legal
- ☐ TOOM - Malpractice-Other
- ☐ TBFM - Fraud/Bad Faith/Misrepresentation
- ☐ TOXX - Other: _____

TORTS: PERSONAL INJURY
- ☐ TOPE - Personal Property
- ☐ TORE - Real Property

OTHER CIVIL FILINGS
- ☐ ABAN - Abandoned Automobile
- ☐ ACCT - Account & Nonmortgage
- ☐ APAA - Administrative Agency Appeal
- ☐ ADPA - Administrative Procedure Act
- ☐ ANPS - Adults in Need of Protective Service

OTHER CIVIL FILINGS (cont'd)
- ☐ MSXX - Birth/Death Certificate Modification/Bond Forfeiture Appeal/ Enforcement of Agency Subpoena/Petition to Preserve
- ☐ CVRT - Civil Rights
- ☐ COND - Condemnation/Eminent Domain/Right-of-Way
- ☐ CTMP - Contempt of Court
- ☐ CONT - Contract/Ejectment/Writ of Seizure
- ☐ TOCN - Conversion
- ☐ EQND - Equity Non-Damages Actions/Declaratory Judgment/ Injunction Election Contest/Quiet Title/Sale For Division
- ☐ CVUD - Eviction Appeal/Unlawful Detainer
- ☐ FORJ - Foreign Judgment
- ☐ FORF - Fruits of Crime Forfeiture
- ☐ MSHC - Habeas Corpus/Extraordinary Writ/Mandamus/Prohibition
- ☐ PFAB - Protection From Abuse
- ☐ EPFA - Elder Protection From Abuse
- ☐ QTLB - Quiet Title Land Bank
- ☐ FELA - Railroad/Seaman (FELA)
- ☐ RPRO - Real Property
- ☐ WTEG - Will/Trust/Estate/Guardianship/Conservatorship
- ☐ COMP - Workers' Compensation
- ☐ CVXX - Miscellaneous Circuit Civil Case

ORIGIN: F ☑ INITIAL FILING; A ☐ APPEAL FROM DISTRICT COURT; O ☐ OTHER; R ☐ REMANDED; T ☐ TRANSFERRED FROM OTHER CIRCUIT COURT

HAS JURY TRIAL BEEN DEMANDED? ☑ YES ☐ NO

Note: Checking "Yes" does not constitute a demand for a jury trial. (See Rules 38 and 39, Ala.R.Civ.P, for procedure)

RELIEF REQUESTED: ☑ MONETARY AWARD REQUESTED ☐ NO MONETARY AWARD REQUESTED

ATTORNEY CODE: MAN057

8/20/2025 1:21:03 PM
Date

/s/ JONATHAN S. MANN
Signature of Attorney/Party filing this form

MEDIATION REQUESTED: ☐ YES ☐ NO ☑ UNDECIDED

Election to Proceed under the Alabama Rules for Expedited Civil Actions: ☐ YES ☑ NO

ELECTRONICALLY FILED
8/20/2025 1:21 PM
68-CV-2025-900681.00
CIRCUIT COURT OF
JEFFERSON COUNTY, ALABAMA
KAREN DUNN BURKS, CLERK

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
BESSEMER DIVISION

JEVON WORRELL, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	**Case No.:**
v.	)	
ROBBIE D. WOOD, INC.,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CLASS ACTION COMPLAINT

Jevon Worrell ("Plaintiff"), through his attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Robbie D. Wood, Inc. ("Robbie D. Wood" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to his own actions, counsel's investigations, and facts of public record.

INTRODUCTION

1. This is a civil action seeking monetary damages and injunctive and declaratory relief from Defendant Robbie D. Wood, arising from its failure to safeguard certain Personally Identifying Information ("PII") and protected health information ("PHI") (collectively "Private Information") of thousands of its current and former employees, resulting in Defendant's network systems being accessed by unauthorized actors.

2. According to Defendant's Breach Notice, on October 1, 2024, Robbie D. Wood

"became aware of unauthorized activity on its computer network" and "an unauthorized individual accessed data within its network." A copy of Plaintiff's Breach Notice is attached as **Exhibit A.**

3. The compromised Private Information included date of birth, Social Security number, driver's license number, financial account information, passport number, medical information, health insurance information, and/or account username and password.[1]

4. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's Private Information. In short, Defendant's failures placed the Class's Private Information in a vulnerable position—rendering them easy targets for cybercriminals.

5. On or around February 11, 2025–more than *four months* after the Data Breach first occurred–Robbie D. Wood finally began notifying Class Members about the Data Breach ("Breach Notice").

6. Plaintiff is a Data Breach victim. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

7. The exposure of one's Private Information to cybercriminals is a bell that cannot be unrung. Before this data breach, Defendant's current and former employees' Private Information was exactly that—private. Not anymore. Now, their Private Information is forever exposed and unsecure.

PARTIES

8. Plaintiff Jevon Worrell is a natural person and citizen of Gainesville, Florida, where

[1] Notice of Data Security Incident, Robbie D. Wood, https://robbiedwood.com/notices/ (last visited August 19, 2025).

he intends to remain.

9. Defendant, Robbie D. Wood, Inc., is an Alabama corporation headquartered at 1051 Old Warrior River Rd., Dolomite, AL.

JURISDICTION AND VENUE

10. Jurisdiction is proper in Alabama because, at all relevant times, Robbie D. Wood conducted (and continues to conduct) business in Alabama, Plaintiff provided his Private Information to Robbie D. Wood in Alabama, Plaintiff's Private Information was stored on Robbie D. Wood's computer networks, systems and/or servers in Alabama, many of Robbie D. Wood's wrongful acts and omissions took place in Alabama, and Defendant's principal place of business is in Alabama.

11. Venue is proper in Jefferson County, Alabama pursuant to Ala. Code §§ 6-3-7(a)(1) and (2) because, at all relevant times, Defendant's principal place of business is in Jefferson County, because a substantial part of the events or omissions giving rise to this action occurred in Jefferson County, and Defendant routinely conducts business throughout Jefferson County.

FACTUAL ALLEGATIONS

Robbie D. Wood

12. Robbie D. Wood touts itself as a "front runner in hazardous waste transportation and chemical product transportation" with locations in North Carolina, Alabama, and Texas.[2]

13. On information and belief, Robbie D. Wood failed to undertake adequate measures to safeguard the Private Information of Plaintiff and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

[2] Home, Robbie D. Wood, https://robbiedwood.com/ (last visited August 19, 2025).

14. In collecting and maintaining the Private Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class members themselves took reasonable steps to secure their Private Information.

15. Under state and federal law, businesses like Defendant have duties to protect their current and former employees' Private Information and to notify them about breaches.

16. Defendant recognizes these duties, declaring in its Breach Notice that the "privacy and security of your information is important to us, and we will continue to take steps to protect information in our car." Ex. A.

17. As a direct and proximate result of Defendant's failures to protect Plaintiff's and the Class Members' sensitive personal information and warn them promptly and fully about the Data Breach, Plaintiff and the proposed Class have suffered widespread injury and damages necessitating Plaintiff seeking relief on a class wide basis.

Plaintiff and the Class Members entrusted their Private Information to Robbie D. Wood

18. Plaintiff and the Class are current and former Robbie D. Wood employees.

19. As a condition of employment with Robbie D. Wood, Plaintiff and the Class Members were required by Robbie D. Wood to provide their sensitive and confidential Private Information, including, but not limited to, their date of birth, Social Security number, driver's license number, financial account information, passport number, medical information, health insurance information, and/or account username and password.[3]

20. Robbie D. Wood maintains records of its employees' Private Information in the ordinary course of business. These records are stored on Robbie D. Wood's network systems.

---

[3] Notice of Data Security Incident, Robbie D. Wood, https://robbiedwood.com/notices/ (last visited August 19, 2025).

21. Upon information and belief, Defendant maintains employee information after the employment relationship has been terminated.

22. Robbie D. Wood acquired, collected, and stored a massive amount of said Private Information of its employees, including Plaintiff and the Members of the proposed Class, which it stored in its electronic systems.

23. By obtaining, collecting, using, and deriving a benefit from its employees' Private Information, Robbie D. Wood assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their Private Information from unauthorized disclosure.

24. Plaintiff has taken reasonable steps to maintain the confidentiality of his Private Information. Plaintiff, as a former employee, relied on Robbie D. Wood to keep his Private Information confidential and securely maintained, to use this information for authorized purposes and disclosures only.

25. Plaintiff and the proposed Class Members entrusted their Private Information to Robbie D. Wood solely for the purposes of applying for employment with Defendant and/or as a condition of employment, with the expectation and implied mutual understanding that Robbie D. Wood would strictly maintain the confidentiality of the information and undertake adequate measures to safeguard it from theft or misuse.

26. Plaintiff and the proposed Class Members would not have entrusted Robbie D. Wood with their highly sensitive Private Information if they had known that Robbie D. Wood would fail to take adequate measures to protect it from unauthorized use or disclosure.

Plaintiff's and the Class Members' Private Information was Improperly Disclosed and Compromised in the Data Breach

27. As a prerequisite to employment, Plaintiff and the Class Members disclosed their

non-public and sensitive Private Information to Robbie D. Wood, with the implicit understanding that their Private Information would be kept confidential. This understanding was based on all the facts and circumstances attendant to their employment there, and the express, specific, written representations made by Robbie D. Wood and its agents.

28. Plaintiff and the Class Members reasonably relied upon Robbie D. Wood's representations to their detriment and would not have provided their sensitive Private Information to Robbie D. Wood if not for Robbie D. Wood's explicit and implicit promises to adequately safeguard that information.

29. According to its Breach Notice, on October 1, 2024, Robbie D. Wood "became aware of unauthorized activity on its computer network." Ex. A.

30. Defendant's investigation into the incident "confirmed an unauthorized individual accessed data within its network," giving cybercriminals unfettered access to its system for an unknown period of time. Ex. A.

31. And, "the information impacted may include individuals' first and last name in combination with one or more of the following data elements: date of birth, Social Security number, driver's license number, financial account information, passport number, medical information, health insurance information, and/or account username and password."[4]

32. Despite this, Defendant waited until February 11, 2025—more than *four months* after the Data Breach began—to begin notifying victims that their Private Information had been compromised and stolen during the Data Breach. *See* Exhibit A.

33. Defendant represented in its Breach Notice that it has "reset passwords, secured all accounts, and conducted a full investigation into the incident." Ex. A. However, this is too little

[4] *Id.*

too late because these precautionary measures should have been taken *before* the Data Breach.

34. Robbie D. Wood's Breach Notice acknowledged the increased risk faced by victims of the Data Breach when it urged those affected to sign up for credit monitoring and recommended that victims "remain vigilant of incidents of fraud and identity theft by reviewing credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors." Ex. A.

35. Although Robbie D. Wood offered several months of complimentary credit monitoring, this is insufficient to address the lifelong risk that victims now face due to the Data Breach.

36. As a result of this Data Breach, the Private Information of Plaintiff and the proposed Class Members was unauthorizedly disclosed and compromised in the Data Breach.

37. The Data Breach was preventable and a direct result of Robbie D. Wood's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' Private Information.

38. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[5]

39. Thus, on information and belief, Plaintiff's and the Class's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

---

[5] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

Plaintiff's Experiences and Injuries

40. Plaintiff Jevon Worrell is a former employee of Defendant and a current subcontractor for Defendant.

41. As a condition of employment, Defendant required Plaintiff to provide it with his Private Information. Defendant thus obtained and maintained Plaintiff's Private Information.

42. Plaintiff provided his Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to Robbie D. Wood's internal policies as well as state and federal law.

43. As a result, Plaintiff was injured by Defendant's Data Breach.

44. Plaintiff received a Notice of Data Breach dated February 11, 2025.

45. Through its Data Breach, Defendant compromised Plaintiff's Private Information including his name, date of birth, Social Security number, driver's license number, password, and username. Ex. A.

46. On information and belief, Plaintiff's Private Information was obtained by cybercriminals and has been, or will be, published on the dark web.

47. Indeed, following the Data Breach, Plaintiff received a prepaid card with directions on how to send money to friends and family in Mexico.

48. Additionally, since the Data Breach, Plaintiff has experienced a large influx of spam calls on his business line. This further demonstrates that Plaintiff's information was stolen in the Data Breach has been placed in the hands of cybercriminals.

49. Once an individual's Private Information is for sale and access on the dark web, as Plaintiff's Private Information is here as a result of the Breach, cybercriminals are able to use

the stolen and compromised to gather and steal even more information.[6] On information and belief, the fraud and spam calls and messages Plaintiff is experiencing are a result of the Data Breach.

50. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

51. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

52. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

53. Plaintiff suffered actual injury from the exposure and theft of his Private Information— which violates his rights to privacy.

54. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

55. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

56. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of

---

[6] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited August 19, 2025).

time and money to try and mitigate his injuries.

57. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

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

58. Because of Defendant's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their Private Information is used;

b. diminution in value of their Private Information;

c. compromise and continuing publication of their Private Information;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen Private Information; and

h. continued risk to their Private Information—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the Private Information.

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

60. The value of Plaintiff and Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"— further exposing the information.

61. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

62. One way that criminals profit from stolen Private Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross- referencing and combining two sources of data—first the stolen Private Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

63. The development of "Fullz" packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

64. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information 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 Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class members' stolen Private

Information is being misused, and that such misuse is fairly traceable to the Data Breach.

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

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

Consumers Prioritize Data Security

67. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[7] Therein, Cisco reported the following:

> a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[8]

---

[7] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited August 19, 2025).

[8] *Id.* at 3.

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[9]

c. 89% of consumers stated that "I care about data privacy."[10]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[11]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[12]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[13]

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

68. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

69. Recently, there has been a high volume of cyberattacks on the freight and transportation industry and Defendant was, or should have been, well aware of such threats.

70. Data thieves regularly target companies like Defendant due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

71. In 2023 alone, the transportation industry suffered 101 data breaches. The number

---

[9] *Id.*
[10] *Id.* at 9.
[11] *Id.*
[12] *Id.*
[13] *Id.* at 11.

of cases rose more than 181% from the year before and the 101 incidents logged in 2023 matches the total number of cases from 2020, 2021 and 2022 combined. In all the segments ranked by SOAX, a data extraction platform used by leading companies to collect and leverage public data, no other industry saw a year-over-year increase larger than transportation, with only the financial services sector coming close (177%).[14]

72. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that ***"[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data*** if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[15]

73. Additionally, in April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that ***"[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies***. They breach networks, use specialized tools to maximize damage, ***leak corporate information on dark web portals***, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[16]

74. The FBI also published multiple public service announcements warning employers of email phishing schemes targeting online employee payroll accounts and sensitive data

---

[14] Jason Cannon, *Transportation at top 10 target of cyberattackers, cases nearly triple last year* CCJ (July 8, 2024) (hereinafter, "Cannon, *Transportation a top 10 target of cyberattackers, cases nearly triple last year*") available at https://www.ccjdigital.com/print/content/15678050 (last visited August 19, 2025).

[15] https://www.cisa.gov/stopransomware/ransomware-guide.

[16] *IRCG-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities* America's Cyber Defense Agency (Dec. 18, 2024) available at: IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities | CISA (last visited August 19, 2025).

associated therewith.[17]

75. This multitude of readily available and accessible information, warnings, and public service announcements confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting, and ferociously aggressive in their pursuit of freight and transportation companies such as Defendant, (ii) cybercriminals were leaking corporate information on dark web portals, and (iii) cybercriminals' tactics included threatening to release stolen data.

76. In light of the information readily available and accessible on the internet and elsewhere before the Data Breach, Defendant, having elected to store the unencrypted Private Information of Plaintiff and Class Members in an internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

77. Further, Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store Private Information and other sensitive information, like Defendant, preceding the date of the breach.

78. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.[18] Of the 3,205 recorded data compromises, 809 of them, or

---

[17] *FBI Warns Employers About Phishing E-Mails Targeting Payroll* (Oct. 10, 2018), available at https://hrdailyadvisor.blr.com/2018/10/10/fbi-warns-employers-about-phishing-e-mails-targeting-payroll/ (last visited Jan. 14, 2024).

[18] *See 2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024); https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf .

25.2% were in the medical or healthcare industry.[19] The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.[20] The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.[21]

79. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

80. Additionally, as companies became more dependent on computer systems to run their business,[22] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[23]

81. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiff and Class members,

---

[19] *Id.*

[20] *Id.*

[21] *Id.*

[22] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[23] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members as a result of a breach.

82. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

83. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

84. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

85. According to the *2023 Annual Data Breach Report*, the number of data compromises in 2023 nearly doubled compared to 2022.[24] And in 2023, a record 3,205 breaches occurred, exposing the data of approximately 353,027,892 victims.[25]

86. And, in 2024, there were 3,158 data breaches with 1,350,835,988 victim notices, a 211% increase year over year.[26]

---

[24] https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ (last visited August 19, 2025).
[25] *Id.*
[26] *2024 Data Breach Report* at 6, Identity Theft Resource Center (Jan. 2025), https://www.idtheftcenter.org/wpcontent/uploads/2025/02/ITRC_2024DataBreachReport.pdf (last visited August 12, 2025).

87. Cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack.[27]

88. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant Failed to Follow FTC Guidelines

89. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

90. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[28] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

---

[27] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[28] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

91. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

92. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

93. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure— to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

94. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

95. Pursuant to Rule 23 of the Alabama Rules of Civil Procedure, Plaintiff brings this class action on behalf of himself and the following class of similarly situated individuals:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach discovered by Robbie D. Wood in October 2024, including all those individuals who received notice of the breach.

96. Excluded from the Class are Robbie D. Wood and its subsidiaries and affiliates, officers, directors, and members of their immediate families, and any entity in which it has a controlling interest, the legal representatives, heirs, successors or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

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

98. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

99. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Although the precise number of individuals is currently unknown to Plaintiff and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

100. Typicality. Plaintiff's claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

101. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

102. Policies Generally Applicable to the Class. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

103. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's Private Information;

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

c. if Defendant were negligent in maintaining, protecting, and securing Private Information;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's Private Information;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

104. Superiority and Manageability. The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds or thousands of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

105. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be

unnecessary and duplicative of this litigation.

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

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

108. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

109. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

110. Likewise, particular issues under Rule 23(c)(2) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;

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

c. Whether Defendant's security measures to protect their data systems were

reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence and/or wantonness;

e. Whether Defendant failed to take commercially reasonable steps to safeguard their employees' Private Information; and,

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

111. Plaintiff re-alleges and incorporates by reference paragraphs 1-110, as if fully set forth herein.

112. Plaintiff and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

113. Defendant owed a duty of care to Plaintiff and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach. And here, that foreseeable danger came to pass.

114. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if their Private Information was wrongfully disclosed.

115. Defendant owed these duties to Plaintiff and Class members 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 practices. After all, Defendant actively sought and obtained Plaintiff and Class members' Private Information.

116. Defendant owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their Private Information.

117. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class members to take appropriate measures to protect their Private Information, 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.

118. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

119. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiff and the Class

involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

120. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining employment from Defendant.

121. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant held vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information—whether by malware or otherwise.

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

123. Defendant improperly and inadequately safeguarded the Private Information of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

124. Defendant breached these duties as evidenced by the Data Breach.

125. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' Private Information by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

126. 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 Private Information of Plaintiff and Class members which actually and proximately caused the Data Breach and Plaintiff and Class members' injury.

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

128. Defendant has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

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

130. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, 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 CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

131. Plaintiff re-alleges and incorporates by reference paragraphs 1-110, as if fully set forth herein.

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

133. 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' Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's Private Information.

134. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

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

136. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant collected

and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

137. 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 the Class.

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

139. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) Plaintiff's Private Information being disseminated on the dark web, according to Experian; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

140. Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

141. Plaintiff re-alleges and incorporates by reference paragraphs 1-110, as if fully set forth herein.

142. Plaintiff and Class members were required to provide their Private Information to Defendant as a condition of receiving employment from Defendant. Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's employment.

143. Plaintiff and Class members reasonably understood that a portion of the funds generated by their employment would be used to pay for adequate cybersecurity measures.

144. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

145. Plaintiff and the Class members accepted Defendant's offers by disclosing their Private Information to Defendant in exchange for employment.

146. In turn, and through internal policies, Defendant agreed to protect and not disclose the Private Information to unauthorized persons.

147. In its Privacy Policy, Defendant represented that it had a legal duty to protect Plaintiff's and Class Member's Private Information.

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

149. After all, Plaintiff and Class members would not have entrusted their Private Information to Defendant in the absence of such an agreement with Defendant.

150. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

151. The covenant of good faith and fair dealing is an element of every contract. Thus, 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—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

153. Defendant materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic Private Information that Defendant created, received, maintained, and transmitted.

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

155. Defendant's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

156. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

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

157. Plaintiff re-alleges and incorporates by reference paragraphs 1-110, as if fully set forth herein.

158. This claim is pleaded in the alternative to the breach of implied contract claim.

159. Plaintiff and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) the revenues generated from Plaintiff and the Class's employment and (2) using their Private Information to provide employment and facilitate its business operations.

160. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class members. And Defendant benefited from the revenue generated by Plaintiff and the Class's employment and from receiving Plaintiff's and Class members' Private Information, as this was used to provide employment and facilitate its business operations.

161. Plaintiff and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

162. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information.

163. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

164. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class members' employment because Defendant failed to adequately protect their Private Information.

165. Plaintiff and Class members have no adequate remedy at law.

166. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Defendant and 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 necessary to protect the interests of Plaintiff and the Class;

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

D. Enjoining Defendant from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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 other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Dated: August 20, 2025

/s/ Jon Mann

Jonathan S. Mann (MAN057)
Austin B. Whitten (WHI165)
PITTMAN, DUTTON, HELLUMS, BRADLEY & MANN, P.C.
2001 Park Place North, Suite 1100
Birmingham, AL 35203
Tel: (205) 322-8880
Email: jonm@pittmandutton.com
Email: austinw@pittmandutton.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Tel: (872) 263-1100
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and the Proposed Class

**Pro Hac Vice* application forthcoming

REQUEST FOR SERVICE

Pursuant to Alabama Rules of Civil Procedure, 4.1 and 4.2, Plaintiff requests that the foregoing Summons & Complaint be served by certified mail.

/s/ Jon Mann
Of Counsel

PLEASE SERVE DEFENDANT BY CERTIFIED MAIL AS FOLLOWS:

Robie D. Wood, Jr.
Robbie D. Wood, Inc.
1051 Old Warrior River Road
Dolomite, AL 35061

EXHIBIT A

=ROBBIE D. WOOD=

25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Jevon Worrell
[redacted]
817

February 11, 2025

Dear Jevon Worrell:

Robbie D. Wood, Inc. ("Robbie D. Wood") writes to inform you of a recent event at Robbie D. Wood. Certain information related to you may have been impacted by this event. This letter includes information about the event, our response, and resources we are making available to you.

What Happened? On October 1, 2024, we became aware of unauthorized activity on our computer network and immediately engaged third-party forensic specialists to determine the full nature and scope of the incident. This investigation confirmed an unauthorized individual accessed data within the Robbie D. Wood network. We then began a thorough review of the impacted portions of our network to determine the type of information contained therein and to whom the information related. Robbie D. Wood completed its review on January 16, 2025, and determined information related to you was impacted.

What Information Was Involved? We have determined the information impacted may include your name in combination with your date of birth, Social Security Number, driver's license number, password and username.

What We Are Doing. In response to this event, Robbie D. Wood reset passwords, secured all accounts, and conducted a full investigation into the incident. Additionally, in an abundance of caution, Robbie D. Wood is offering you access to 12 months of credit monitoring and identity protection services at no cost to you. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed.

What You Can Do. Robbie D. Wood recommends that you remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. Additionally, you can enroll to receive the complimentary credit monitoring and identity protection services we are making available to you. You can also review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information. We understand you may have questions about this incident. You may call 888-802-9713 between Monday through Friday, 9 am to 9 pm ET (excluding holidays) or write to us at 1051 Old Warrior River Road, Dolomite, AL 35061.

DOCUMENT 2

Robbie D. Wood sincerely regrets any concern this incident may cause you. The privacy and security of your information is important to us, and we will continue to take steps to protect information in our care.

Sincerely,

Robbie D. Wood, Inc.

State of Alabama Unified Judicial System Form C-34 Rev. 7/2023	**SUMMONS** **- CIVIL -**	**Court Case Number** 68-CV-2025-900681.00

IN THE CIRCUIT COURT OF JEFFERSON COUNTY, ALABAMA
JEVON WORRELL V. ROBBIE D. WOOD, INC.

NOTICE TO: ROBBIE D. WOOD, INC., 1051 OLD WARRIOR RIVER RD, DOLOMITE, AL 35061
(Name and Address of Defendant)

THE COMPLAINT OR OTHER DOCUMENT WHICH IS ATTACHED TO THIS SUMMONS IS IMPORTANT, AND YOU MUST TAKE IMMEDIATE ACTION TO PROTECT YOUR RIGHTS. YOU OR YOUR ATTORNEY ARE REQUIRED TO FILE THE ORIGINAL OF YOUR WRITTEN ANSWER, EITHER ADMITTING OR DENYING EACH ALLEGATION IN THE COMPLAINT OR OTHER DOCUMENT, WITH THE CLERK OF THIS COURT. A COPY OF YOUR ANSWER MUST BE MAILED OR HAND DELIVERED BY YOU OR YOUR ATTORNEY TO THE PLAINTIFF(S) OR ATTORNEY(S) OF THE PLAINTIFF(S), JONATHAN S. MANN
[Name(s) of Attorney(s)]

WHOSE ADDRESS(ES) IS/ARE: 2001 PARK PLACE N., STE. 1100, BIRMINGHAM, AL 35203
[Address(es) of Plaintiff(s) or Attorney(s)]

THIS ANSWER MUST BE MAILED OR DELIVERED WITHIN 30 DAYS AFTER THIS SUMMONS AND COMPLAINT OR OTHER DOCUMENT WERE SERVED ON YOU OR A JUDGMENT BY DEFAULT MAY BE RENDERED AGAINST YOU FOR THE MONEY OR OTHER THINGS DEMANDED IN THE COMPLAINT OR OTHER DOCUMENT.

TO ANY SHERIFF OR ANY PERSON AUTHORIZED BY THE ALABAMA RULES OF CIVIL PROCEDURE TO SERVE PROCESS:

☐ You are hereby commanded to serve this Summons and a copy of the Complaint or other document in this action upon the above-named Defendant.

☑ Service by certified mail of this Summons is initiated upon the written request below of JEVON WORRELL *[Name(s)]* pursuant to the Alabama Rules of the Civil Procedure.

08/20/2025 *(Date)* /s/ KAREN DUNN BURKS *(Signature of Clerk)* By: _____ *(Name)*

☑ Certified Mail is hereby requested. /s/ JONATHAN S. MANN *(Plaintiff's/Attorney's Signature)*

RETURN ON SERVICE

Certified Mail

☐ Return receipt of certified mail received in this office on _____ *(Date)*.

Personal/Authorized

☐ I certify that I personally delivered a copy of this Summons and the Complaint or other document to _____ *(First and Last Name of Person Served)* in _____ *(Name of County)* County, Alabama on _____ *(Date)*.

Document left:

☐ with above-named Defendant;
☐ with an individual authorized to receive service of process pursuant to Rule 4(c), Alabama Rules of Civil Procedure;
☐ at the above-named Defendant's dwelling house or place or usual place of abode with some person of suitable age and discretion then residing therein.

Return of Non-Service

☐ I certify that service of process of this Summons and the Complaint or other document was refused by _____ *(First and Last Name of Person Served)* in _____ *(Name of County)* County, Alabama on _____ *(Date)* who is:

☐ the above-named Defendant;
☐ an Individual authorized to receive service of process pursuant to Rule 4(c), Alabama Rules of Civil Procedure;

☐ As a designated process server pursuant to Rule 4(i)(1)(B), Alabama Rules of Civil Procedure, I certify that I am at least 19 years of age, I am not a party to this proceeding, and I am not related within the third degree by blood or marriage to the party seeking service of process.

_____ *(Type of Process Server)* _____ *(Server's Signature)* _____ *(Address of Server)*

_____ *(Badge or Precinct Number of Sheriff or Constable)* _____ *(Server's Printed Name)*

_____ *(Badge or Precinct Number of Sheriff or Constable)* _____ *(Telephone Number of Designated Process Server)*

Service Return Copy