Service of Process Transmittal Summary

TO: Kent J Pagel, Attorney
Pagel Davis & Hill Pc
1415 Louisiana St Fl 22
Houston, TX 77002-7344

RE: **Process Served in Texas**

FOR: Trussway Manufacturing, LLC (Domestic State: TX)

ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:

TITLE OF ACTION:	LORENZO FLORES and SIMBA FLORES on behalf of themselves and all others similarly situated vs. TRUSS WAY MANUFACTURING, LLC
CASE #:	423CV02509
PROCESS SERVED ON:	C T Corporation System, Dallas, TX
DATE/METHOD OF SERVICE:	By Process Server on 07/13/2023 at 15:16
JURISDICTION SERVED:	Texas
ACTION ITEMS:	CT will retain the current log Image SOP Email Notification, Kent J Pagel kjp@pdhlaw.com
REGISTERED AGENT CONTACT:	C T Corporation System 1999 Bryan Street Suite 900 Dallas, TX 75201 866-539-8692 CorporationTeam@wolterskluwer.com

Wolters Kluwer

PROCESS SERVER DELIVERY DETAILS

Date: Thu, Jul 13, 2023
Server Name: Tracy Edwards

Entity Served	TRUSSWAY MANUFACTURING, LLC
Case Number	4:23-CV-02509
Jurisdiction	TX

Inserts		

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Southern District of Texas

LORENZO FLORES and SIMBA FLORES on behalf of themselves and all others similarly situated,

Plaintiff(s)

v.

TRUSSWAY MANUFACTURING, LLC

Defendant(s)

Civil Action No. 4:23-cv-02509

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* TRUSSWAY MANUFACTURING, LLC
C/O CT Corporation
1999 Bryan Street, Suite 900
Dallas, Texas 75201

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Joe Kendall
Kendall Law Group, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, TX 75219

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Date: July 12, 2023

Nathan Ochsner, Clerk of Court

s/ Rhonda Moore-Konieczny
Signature of Clerk or Deputy Clerk

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. 4:23-cv-02509

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____

was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____

_____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____

_____ , a person of suitable age and discretion who resides there,

on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is

designated by law to accept service of process on behalf of *(name of organization)* _____

_____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____

Server's signature

_____

Printed name and title

_____

Server's address

Additional information regarding attempted service, etc:

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

LORENZO FLORES and **SIMBA FLORES** on behalf of themselves and all others similarly situated, *Plaintiffs*,	§	**Case No.: 4:23-cv-02509**
v.	§	
TRUSSWAY MANUFACTURING, LLC, *Defendant.*	§	**JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Lorenzo Flores and Simba Flores ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members"), bring this Class Action Petition against Defendant Trussway Manufacturing, LLC (hereinafter "Trussway" or "Defendant"), a Texas limited liability company. Plaintiffs seek damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of the recent targeted cyberattack against Defendant that allowed a third party to access Defendant's computer systems and data, resulting in the compromise of highly sensitive personal information (the "Data Breach"). Because of the Data Breach, Plaintiffs and Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their sensitive personal information.

2. Upon information and belief, the information compromised in the Data Breach is

confidential personally identifiable information (PII) and personal health information of Defendant's current and former employees (collectively the "Private Information").

3. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their Private Information had been subject to the unauthorized access of an unknown third party or precisely what specific type of information was accessed.

4. On information and belief, Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to a cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

5. In addition, on information and belief, Defendant failed to properly monitor the computer network and IT systems that contained the Private Information.

6. Plaintiffs' and Class Members' identities are now at imminent risk because of Defendant's negligent conduct—since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

7. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *inter alia*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing

fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

8. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now—and in the future—closely monitor their financial accounts to guard against identity theft.

9. Plaintiffs and Class Members may also incur out of pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

10. By their Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach.

11. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

12. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (1) negligence, (2) breach of implied contract; (3) negligence per se; (4) breach of fiduciary duty; (5) intrusion upon seclusion/invasion of privacy and (6) unjust enrichment.

PARTIES

13. Plaintiff Lorenzo Flores is a natural person and a citizen of the State of Colorado. He resides in Colorado Springs, Colorado and has no intention of moving to a different state in the

immediate future.

14. Plaintiff Simba Flores is a natural person and a citizen of the State of Colorado. She resides in Colorado Springs, Colorado and has no intention of moving to a different state in the immediate future.

15. Defendant is a Texas limited liability company with its headquarters and principal place of business located at 9411 Alcorn, Houston, Texas 77093. The registered agent for service of process is CT Corporation, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d)(2), because this is a class action involving more than one hundred putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiffs (and many members of the class) are citizens of states different than Defendant.

17. This Court has general personal jurisdiction over Defendant because Defendant principal place of business and headquarters are in Houston Texas. And moreover, Defendant regularly conducts substantial business in Texas.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within the Houston Division of the Southern District of Texas, and Defendant conducts substantial business and is headquartered in the Houston Division of the Southern District of Texas.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the Private Information of Plaintiffs and Class Members

19. Defendant is a manufacturer of floor trusses, roof trusses, and pre-assembled door and window openings.[1] It was founded in 1972 and has over 1,000 employees.[2]

20. In the ordinary course of business, Defendant receives and maintains the Private Information of thousands of current and former employees.

21. Defendant agreed to and undertook legal duties to maintain the Private Information entrusted to it by Plaintiffs and Class Members safely, confidentially, and in compliance with all applicable laws.

22. Defendant held the Private Information of Plaintiffs and Class Members.

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

24. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the Defendant to keep their Private Information confidential and securely maintained, and to make only authorized disclosures of this information.

Defendant's Data Breach

25. Defendant failed in its duties in March 2023, when its inadequate security practices resulted in the Data Breach.[3] Defendant was overwhelmed by a ransomware attack—where criminals access sensitive files, encrypt those files, and then demand ransom payment for the

[1] TRUSSWAY, https://trussway.com/ (last visited July 3, 2023).
[2] *Who We Are*, TRUSSWAY, https://trussway.com/who-we-are/ (last accessed July 3, 2023).
[3] *Data Breach Notice*, attached as **Exhibit A**.

decryption key.[4] Over two months after the start of the Data Breach, May 30, 2023, Defendant admitted that "between March 7, 2023 and April 1, 2023, an unauthorized actor viewed and obtained files stored on certain servicers in our network."[5]

26. Thus, upon information and belief, the Data Breach was the result of a deliberate attempt by criminals to access the Private Information of Plaintiffs and the Class Members.

27. Upon information and belief, thousands of individuals had their Private Information exposed in the Data Breach. Also, upon information and belief, the Private Information exposed was not encrypted. The Private Information included names, addresses, Social Security numbers, dates of birth, and health plan enrollment information.[6] It may have also included health insurance policy numbers, driver's license numbers, passport numbers, other government-issued identification numbers, financial account information, and if an individual had filed a claim for worker's compensation or short-term disability the medical information relating to such claims.[7]

28. Defendant had obligations created by contract law, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

29. Simply put, Defendant failed in its duties when its inadequate security practices caused the Data Breach.

30. Defendant kept the Class in the dark for nearly two months after discovery of the Data Breach—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

---

[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] *Id.*

31. And when it did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach puts them at a present, continuing, and significant risk of suffering identity theft, warning them to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and monitoring free credit reports for any unauthorized activity."[8]

32. Since the breach, Defendant has stated it is "taking steps to enhance our existing security measures, which will include the use of a new managed detection and response platform."[9] But this is too little and too late as the Private Information of Plaintiffs and the Class are already in the hands of criminals.

33. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

34. Defendant's negligence is further evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the Private Information.

35. Defendant has done little to remedy its Data Breach. True, Defendant has offered concessions of credit monitoring and identity services to Plaintiffs and the Class.[10] But upon information and belief, such services do not properly compensate Plaintiffs and Class Members for the injuries that Defendant inflicted upon them.

36. Because of Defendant's Data Breach, the sensitive Private Information of Plaintiffs and Class Members were placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class Members.

Defendant Fails to Comply with FTC Guidelines

[8] *Id.*
[9] *Id.*
[10] *Id.*

37. The Federal Trade Commission ("FTC") promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

38. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[11] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[12]

39. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential Consumer data as an unfair act or

---

[11] *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.

[12] *Id.*

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.

41. Defendant failed to properly implement basic data security practices.

42. Defendant was at all times fully aware of its obligation to protect the Private Information of persons who had provided it to Defendant. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

43. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

44. Other best cybersecurity practices that are standard include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

45. Upon information and belief Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all

established standards in reasonable cybersecurity readiness.

46. These foregoing frameworks are existing and applicable industry standards, and it is believed Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

Defendant Violated HIPAA

47. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[13]

48. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI ("Personal Health Information") is properly maintained.[14]

49. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to

[13] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[14] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures

establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

50. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

Defendant's Negligence

51. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing the means by which the cyberattacks were able to first access Defendant's networks, and to maintain adequate email security practices;

e. Failing to put into place proper procedures, software settings, and data security software protections to adequately protect against a blunt force intrusion;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

g. Failing to comply with HIPAA; and

h. Failing to adhere to industry standards for cybersecurity.

52. As the result of antivirus and malware protection software in dire need of security updating, inadequate procedures for handling phishing emails or emails containing viruses or other malignant computer code, and other failures to maintain its networks in configuration that would protect against cyberattacks, Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's IT systems and remove data which contained unsecured and unencrypted Private Information.

53. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with Defendant.

Data Breaches Cause Disruption and Put Persons at an Increased Risk of Fraud and Identity Theft

54. Data breaches are problematic because the breaches can negatively impact the overall daily lives of individuals affected by the attack.

55. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[15]

56. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, taking over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's

[15] *See GAO-07-737: Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOV. ACCOUNTING OFFICE (2007) https://www.gao.gov/new.items/d07737.pdf.

identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

57. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[16]

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

59. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being

[16] *See IdentityTheft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited July 31, 2022).

issued in the victim's name.

60. Moreover, theft of Private Information results in the loss of a valuable property right.[17]

61. Notably, there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and between when Private Information and/or financial information is stolen and when it is used.

62. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

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

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

65. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

---

[17] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

66. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[18] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

67. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[19] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[20] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

68. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

69. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

---

[18] *See* Ashiq Ja, Hackers *Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited July 31, 2022).

[19] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION (2018) www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 31, 2022).

[20] *Id.* at 4.

70. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

71. Medical information is especially valuable to identity thieves. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016 – the same as a Facebook account.[21] That pales in comparison with the asking price for medical data, which was selling for $50 and up.[22]

72. Because of the value of its collected and stored data, the medical industry has experienced disproportionally higher numbers of data theft events than other industries.

73. For this reason, Defendant knew or should have known about these dangers and strengthened its data security accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

The Experiences—and Injuries—of Plaintiffs and Class Members

74. To date, Defendant has done nothing to provide Plaintiffs and the Class Members with relief for the damages they have suffered as a result of the Data Breach. Defendant has merely offered Plaintiffs and Class Members one year of free credit monitoring. But this does not compensate them for damages incurred and time spent dealing with the Data Breach. Signing up for this service requires Plaintiffs and Class Members to forfeit time that could otherwise be spent making money or enjoying life.

---

[21] *See* Omri Toppol, *Email Security: How You Are Doing It Wrong & Paying Too Much*, LOGDOG (Feb. 14, 2016), https://getlogdog.com/blogdog/email-security-you-are-doing-it-wrong/.

[22] Lisa Vaas, *Cyberattacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SECURITY (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals// (last visited July 1, 2022);

75. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

76. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

77. Plaintiffs and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class Members.

78. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

79. Plaintiffs and Class Members suffered actual injury from having their Private Information compromised as a result of the Data Breach including, but not limited to (i) damage to and diminution in the value of their Private Information, a form of property that Defendant obtained from Plaintiffs and Class Members; (ii) violation of their privacy rights; and (iii) imminent and impending injury arising from the increased risk of identity theft and fraud; and (iv) emotional distress.

80. Plaintiffs and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data

Breach relating to:

a. Reviewing and monitoring financial and other sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

81. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

Plaintiff Lorenzo Flores' Experience

82. Plaintiff Lorenzo Flores ("Mr. Flores") is a former employee of Defendant. He was last employed by Defendant in October 2022.

83. Mr. Flores has suffered directly from the Data Breach. He has noticed several inquiries on his credit and received many fraud alerts. His debit card number was also used at

a gas station for a purchase he did not authorize.

84. In short, it appears that his personal information is being used for a litany of fraudulent activities.

85. As a condition of his employment, Mr. Flores entrusted confidential information such as his name, address, date of birth, Social Security number and other personally identifiable information to Defendant with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents related to him.

86. As a result of the Data Breach, Mr. Flores has made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

87. Mr. Flores suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (i) damage to and diminution in the value of his Private Information—a form of property that Defendant obtained from Plaintiff; (ii) violation of his privacy rights; (iii) the likely theft of his Private Information and (iv) imminent and impending injury arising from the increased risk of identity theft and fraud because of the nature of the compromised private personal information.

88. As a result of the Data Breach, Mr. Flores also suffered emotional distress because of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity theft and fraud. Mr. Flores is concerned about

identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

89. As a result of the Data Breach, Mr. Flores anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Mr. Flores will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

Plaintiff Simba Flores' Experience

90. Plaintiff Simba Flores ("Ms. Flores") is a former employee of Defendant. She was last employed by Defendant in February 2023.

91. Ms. Flores has suffered directly from the Data Breach. For one, she has noticed a fraudulent charge with her debit card number that she did not authorize.

92. And since the breach, Ms. Flores has started receiving spam texts or spam phone calls.

93. As a condition of her employment, Ms. Flores entrusted confidential information such as her name, address, date of birth, Social Security number and other personally identifiable information to Defendant with the reasonable expectation and understanding that Defendant would take, at a minimum, industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify her of any data security incidents related to her.

94. As a result of the Data Breach, Ms. Flores made reasonable efforts to mitigate the impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or medical records for any indications of actual or attempted identity theft or fraud.

95. Ms. Flores suffered actual injury from having her Private Information compromised

as a result of the Data Breach including, but not limited to (i) damage to and diminution in the value of her Private Information—a form of property that Defendant obtained from Plaintiff; (ii) violation of her privacy rights; (iii) the likely theft of her Private Information and (iv) imminent and impending injury arising from the increased risk of identity theft and fraud.

96. As a result of the Data Breach, Ms. Flores also suffered emotional distress because of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using their Private Information for purposes of identity theft and fraud. Plaintiff is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

97. As a result of the Data Breach, Ms. Flores anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

98. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated.

99. Plaintiffs proposes the following Class definition, subject to amendment as appropriate:

> All persons residing in the United States whose information was compromised by the Data Breach—including all persons that Defendant sent a notice of the Data Breach to (the "Nationwide Class").

100. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives,

attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and members of their staff.

101. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification.

102. Numerosity. The Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of thousands of current and former employees whose Private Information was compromised in the Data Breach.

103. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages because of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's conduct was per se negligent;

l. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendant was unjustly enriched;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

104. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

105. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

106. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

107. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

108. 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.

109. Likewise, particular issues 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 public of the Data Breach;

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

c. Whether Defendant's security measures to protect its 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;

e. Whether Defendant failed to take commercially reasonable steps to safeguard the 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.

110. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and All Class Members)

111. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

112. Defendant required Plaintiffs and Class Members to submit non-public personal information in exchange for employment, which Defendant then stored and maintained in its computer networks.

113. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duties included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

114. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

115. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its employees, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a Data Breach or data breach.

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

117. 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.

118. 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.

119. Defendant breached its duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

120. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members.

121. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

122. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

123. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner.

124. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

125. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

126. When Plaintiffs and Class Members provided their Private Information to Defendant in exchange for employment, they entered into implied contracts with Defendant under

which Defendant agreed to reasonably protect such information.

127. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

128. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and were consistent with industry standards.

129. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

130. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

131. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

132. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

133. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged herein, including the loss of the benefit of the bargain.

134. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

135. Plaintiffs and Class Members are also entitled to injunctive relief requiring

Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiffs and All Class Members)

136. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

137. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

138. Pursuant to HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiffs and Class Members' Private Information.

139. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

140. Defendant breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

141. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

142. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

143. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

144. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and All Class Members)

145. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

146. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs and Class Members' Private Information, Defendant became fiduciaries by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (i) for the safeguarding of Plaintiffs and Class Members' Private Information; (ii) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (iii) to maintain complete and accurate records of what information (and where) Defendant did and does store such private and confidential information.

147. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationships with its employees, in particular, to keep secure

the Private Information.

148. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period so that harm might be mitigated.

149. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs and Class Members' Private Information.

150. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

151. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

152. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of

the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

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

FIFTH CAUSE OF ACTION
Intrusion Upon Seclusion/Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

154. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

155. The State of Texas recognizes the tort of Intrusion upon Seclusion, and adopts the formulation of that tort found in the Restatement (Second) of Torts, which states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts§ 652B (1977).

156. Plaintiffs and Class Members had a reasonable expectation of privacy in the Private Information Defendant mishandled.

157. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

158. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and

that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

159. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

160. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

161. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their Private Information without their informed, voluntary, affirmative, and clear consent.

162. The conduct described above was at or directed at Plaintiffs and the Class Members.

163. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

164. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award

of damages on behalf of themselves and the Class.

SIXTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

165. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

166. Plaintiffs bring this claim individually and on behalf of all Class Members. This count is plead in the alternative to the breach of implied contract count.

167. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including earnings made by or on behalf of Plaintiffs and the Class Members or revenue derived from the use of their Private Information.

168. As such, a portion of the payments made by or on behalf of Plaintiffs and the Class Members or derived from their Private Information is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

169. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant with their Private Information and by providing their employment services.

170. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

171. In particular, Defendant enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and

Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

172. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

173. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

174. Defendant acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

175. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

176. Plaintiffs and Class Members have no adequate remedy at law.

177. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity of how their Private Information is used; (c) the compromise, publication, and/or theft of their Private Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (e) lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from fraud and identity theft; (f) the continued risk to their Private Information, which remains in

Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

178. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

179. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members;

D. For an award of damages, including actual, nominal, statutory, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury for any and all issues in this action so triable as of right.

Date: July 10, 2023

Respectfully submitted,

/s/ Joe Kendall
JOE KENDALL
Texas Bar No. 11260700
SDTX Bar No. 30973
KENDALL LAW GROUP, PLLC
3811 Turtle Creek Blvd., Suite 1450
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Samuel J. Strauss*
Raina C. Borrelli*
TURKE & STRAUSS LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Facsimile: (608) 509-4423
raina@turkestrauss.com
sam@turkestrauss.com

ATTORNEYS FOR PLAINTIFFS
****Pro Hac Vice Forthcoming***

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

May 30, 2023

Dear <<Name1>>:

Trussway understands the importance of protecting information. We are writing to inform you that we recently identified and addressed a data security incident involving your information. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

What Happened?
We determined on March 31, 2023 that certain devices in our network were encrypted with ransomware. When we learned of the incident, we immediately implemented our response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm also was engaged. We notified law enforcement and are supporting its investigation.

The evidence showed that between March 7, 2023 and April 1, 2023, an unauthorized actor viewed and obtained files stored on certain servers in our network. We conducted a careful review of the files and, on May 19, 2023, determined that one or more of the files contained your information.

What Information Was Involved?
The file(s) contained your name, address, Social Security number, date of birth, and health insurance plan enrollment information. The files also may have contained your health insurance policy number, driver's license number, passport number, other government-issued identification number, financial account information, and if you filed a claim for workers' compensation or short-term disability, medical information relating to your claim.

What We Are Doing.
We wanted to notify you of this incident and to assure you that we take it seriously. To help prevent something like this from happening again, we have taken and are taking steps to enhance our existing security measures, which will include the use of a new managed detection and response platform.

What You Can Do.
We have arranged for you to receive one year of access to Equifax Complete™ Premier credit monitoring. This product helps detect possible misuse of your information and provides you with identity protection solutions focused on immediate identification and resolution of identity theft. Activating this product will not hurt your credit score. For more information on identity theft prevention and Equifax Complete™ Premier, including instructions on how to activate your one year of access, as well as some additional steps you can take in response, please review the pages that follow this letter.

For More Information.

We regret that this occurred and apologize for any inconvenience. If you have any questions, please contact us at us at 877-281-2135, Monday through Friday, between 8:00 a.m. and 8:00 p.m., Central.

Sincerely,

Trussway Manufacturing

EQUIFAX®

<<Name1>>
Enter your Activation Code: *<<ACTIVATION CODE>>*
Enrollment Deadline: September 30, 2023

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of *<<ACTIVATION CODE>>* then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. *[2]Credit monitoring from Experian and TransUnion will take several days to begin.* *[3]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.* *[4]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* *[5]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co* *[6]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.
How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Trussway is located at 9411 Alcorn Street, Houston, Texas 77093 and can be reached at (713) 691-6900.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.

- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

JS 44 (Rev. 02/19)

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

LORENZO FLORES and SIMBA FLORES on behalf of themselves and all others similarly situated,

(b) County of Residence of First Listed Plaintiff El Paso County
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Joe Kendall, Kendall Law Group, PLLC, 3811 Turtle Creek Blvd., Suite 1450, Dallas, TX 75219, 214/744-3000

DEFENDANTS

TRUSSWAY MANUFACTURING, LLC

County of Residence of First Listed Defendant
(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

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

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

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

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
- ☐ 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:
Data Breach

VII. REQUESTED IN COMPLAINT:

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

DEMAND $

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

VIII. RELATED CASE(S) IF ANY

(See instructions):
JUDGE _____ DOCKET NUMBER _____

DATE
07/10/2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Joe Kendall

FOR OFFICE USE ONLY

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

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

Lorenzo Flores, et al.	§	
Plaintiff,	§	
	§	
v.	§	CIVIL ACTION NO. 4:23-cv-02509
	§	
Trussway Manufacturing, LLC	§	
Defendant.	§	

ORDER FOR CONFERENCE AND DISCLOSURE OF INTERESTED PARTIES

1. Counsel and all parties appearing pro se shall appear for an initial pretrial and scheduling conference before

Magistrate Judge Andrew M Edison
November 1, 2023, at 09:00 AM
by video
United States Courthouse

2. Within fifteen days from receipt of this order, counsel shall file with the clerk a certificate listing all persons, associations of persons, firms, partnerships, corporations, affiliates, parent corporations, or other entities that are financially interested in the outcome of this litigation. If a group can be specified by a general description, individual listing is not necessary. Underline the name of each corporation whose securities are publicly traded. If new parties are added or if additional persons or entities that are financially interested in the outcome of the litigation are identified at any time during the pendency of this litigation, then each counsel shall promptly file an amended certificate with the clerk.

3. NOTICE TO PARTIES ASSERTING FEDERAL JURISDICTION IN DIVERSITY CASES: Under 28 U.S.C. § 1332 there must be complete diversity between plaintiffs and defendants. Complete diversity requires that all persons on one side of the controversy be citizens of different states from all persons on the other side. The party asserting federal jurisdiction in a diversity action has the burden to demonstrate that there is complete diversity. The citizenship of limited liability entities is determined by the citizenship of their members. *Harvey v. Grey Wolf Drilling Co.*, 542 F.3d 1077, 1080 (5th Cir. 2008). When members of a limited liability entity are themselves entities or associations, citizenship must be traced through however many layers of members there are until arriving at the entity that is not a limited liability entity and identifying its citizenship status. *See Mullins v. TestAmerica, Inc.*, 564 F.3d 386, 397 (5th Cir. 2009). If the Complaint or Notice of Removal filed in this action does not show the citizenship of all limited liability entities, the plaintiff (if initiating the action in federal court) or the

defendant (if removing the action from state court) is ORDERED to file an amended complaint or notice of removal, respectively, within twenty days from the entry of this order. The failure to allege facts establishing complete diversity of citizenship may result in dismissal or remand of this action by the court on its own initiative without further notice.

4. Fed. R. Civ. P. 4(m) requires defendant(s) to be served within 90 days after the filing of the complaint. The failure of plaintiff(s) to file proof of service within 90 days after the filing of the complaint may result in dismissal of this action by the court on its own initiative.

5. After the parties confer as required by Fed. R. Civ. P. 26(f), counsel and all parties appearing pro se shall prepare and file, not less than 10 days before the scheduling conference, a joint discovery/case management plan containing the information required on the attached form.

6. The court will enter a scheduling order and may rule on any pending motions at the scheduling conference.

7. Counsel and all parties appearing pro se who file or remove an action must serve a copy of this order with the summons and complaint or the notice of removal.

8. Unless proceeding pro se, each party must be represented by an attorney who has knowledge of the facts and authority to bind the party at the scheduling conference.

9. Prior to the scheduling conference, counsel and all parties appearing pro se shall discuss with their clients and each other whether alternative dispute resolution is appropriate and at the conference advise the court of the results of their discussions.

10. A person proceeding pro se is bound by the requirements imposed upon counsel in this Order.

11. Failure to comply with this order may result in sanctions, including dismissal of the action and assessment of fees and costs.

Court's Procedures: Information on the court's practices and procedures and how to reach court personnel may be obtained at the Clerk's website at www.txs.uscourts.gov or from the intake desk of the Clerk's office.

By Order of the Court

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

_____,	§	
	§	
Plaintiff(s),	§	
	§	
v.	§	Civil Action No. _____
	§	
_____,	§	
	§	
Defendant(s).	§	

JOINT DISCOVERY/CASE MANAGEMENT PLAN UNDER RULE 26(f) FEDERAL RULES OF CIVIL PROCEDURE

(Please restate the instruction before furnishing the information.)

1. State where and when the meeting of the parties required by Rule 26(f) was held, and identify the counsel or self-represented litigant who attended for each party. NOTE: the Rule 26(f) meeting must be held in person, by phone, or by video. Email meetings are not permitted.

2. List the cases related to this one that are pending in any state or federal court, with the case number and court, and state how the cases are related.

3. Briefly describe what this case is about.

4. Identify any issues as to service of process, personal jurisdiction, or venue.

5. Federal jurisdiction.

   a. Specify the allegation of federal jurisdiction.

   b. Identify the parties, if any, who disagree with the plaintiff's federal jurisdictional allegations, and state their reasons.

   c. If federal jurisdiction is based on diversity of citizenship and any of the parties is a limited liability entity, please state the citizenship of each of the members of the limited liability entity. When members of a limited liability entity are themselves entities or associations, citizenship must be traced through however many layers of members there are until arriving at the entity that is not a limited liability and identifying its citizenship.*See Acadian Diagnostic Labs., L.L.C. v. Quality Toxicology, L.L.C.*, 965 F.3d 404, 408 fn.1 (5th Cir. 2020).

6. List anticipated additional parties that should be included, and by whom they are wanted.

7. List anticipated interventions.

8. Describe class-action or collective-action issues.

9. State whether each party has made the initial disclosures required by Rule 26(a). If not, describe the arrangements that have been made to complete the disclosures and the dates.

10. If the case includes a claim for attorneys' fees, state whether the parties agree to submit the fees issue to the court for resolution on affidavits or declarations, after the other issues are resolved.

11. Describe the proposed discovery plan, including:

    a. Responses to the matters raised in Rule 26(f), including any agreements (and disputes) concerning electronic and other discovery.

    b. Any threshold issues–such as limitations, jurisdiction, or immunity–that should be scheduled for early resolution, what discovery targeted to those issues may need to occur early, and how long this targeted discovery will take.

12. Experts

    a. Are experts needed on issues other than attorneys' fees?

    b. If medical experts are needed, identify whether they are only treating physicians or also designated on other issues.

    c. The date the party with the burden of proof on an issue will be able to designate experts and provide the reports required by Rule 26(a)(2)(B).

    d. The date the opposing party will be able to designate responsive experts and provide the reports required by Rule 26(a)(2)(B).

13. State the date discovery can reasonably be completed.

14. If the parties are not agreed on a part of the discovery plan, describe the separate views and proposals of each party.

15. Specify the discovery beyond initial disclosures that has been undertaken to date.

16. Describe the possibilities for a prompt settlement or resolution of the case that were discussed in your Rule 26(f) meeting or have emerged since then.

17. From the attorneys' discussion with the clients, state the alternative dispute resolution techniques that are reasonably suitable and when they are likely to be effective in this case.

18. With the consent of all parties, United States Magistrate Judge Andrew Edison may preside and hear jury and non-jury trials. Indicate the parties' joint position on a trial before Judge Edison.

19. State whether a jury demand has been made and if it was made on time.

20. Specify the number of hours it will likely take to present the evidence.

21. List pending motions that may be ruled on at the initial pretrial and scheduling conference.

22. List other pending motions.

23. List issues or matters, including discovery, that should be addressed at the conference.

24. Certify that all parties have filed Disclosure of Interested Parties as directed in the Order for Conference and Disclosure of Interested Parties, listing the date of filing for original and any amendments. DO NOT STATE THAT THE DISCLOSURE OF INTERESTED PARTIES WILL BE FILED IN THE FUTURE.

_____ _____

Counsel for Plaintiff(s) Date

_____ _____

Counsel for Defendant(s) Date