UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

JAMES MORRISON, on behalf of himself and all others similarly situated, Plaintiff, v. ENTRUST CORPORATION and ENTRUST MN CORPORATION, Defendants.	Case No. 0:23-cv-415 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiff James Morrison ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, bring this class action against Entrust Corporation and Entrust MN Corporation ("Entrust" or "Defendants"), upon personal knowledge as to himself and his own acts and experiences, and upon information and belief as to all other matters, including his counsel's investigation, allege as follows. Plaintiff believes that additional evidentiary support exists for his allegations, given an opportunity for discovery.

INTRODUCTION AND NATURE OF ACTION

1. Entrust is a cybersecurity vendor providing services including securing transactions, identifies, and data that promote "trust and confidence" to various types of business and government entities.

2. Because it specializes in cybersecurity, Entrust is responsible for managing and overseeing highly sensitive data. Entrust and its clients collect, store, and use personal and confidential information that includes names, addresses, social security numbers, medical records

and histories, and financial account information. As Entrust itself acknowledged, this type of personal and sensitive data is highly targeted by hackers seeking to exploit that data for nefarious purposes. For example, fraudsters utilize financial information to make fraudulent transactions and purchases or use a collection of personal data to take out fraudulent loans. In the wrong hands, these types of sensitive, personal data may be wielded to cause significant harm to the individual whose information is described in the records that Entrust, through its clients and as an employer, stores.

3. Entrust assures its clients and employees that it is a sophisticated cybersecurity company capable of keeping private information safe. In fact, Entrust touts that the "world's most entrusted organizations trust us" and that they are "a pioneer in the business of securing transactions" that is "actively involved in defining industry standards and best practices".[1] Entrust also frequently published cybersecurity-related webinars stressing the importance of maintaining adequate data security and offering advice on how to keep data safe and prevent a data breach. [2]

4. Indeed, Entrust has provided cybersecurity services for organizations for over 50 years, and has offices and data centers in Minneapolis, Texas, Colorado, and Florida. It is, moreover, a sophisticated company with approximately 2,500 current employees across its locations, and its cyber services generate $4.35 million dollars in sales.[3]

5. In reality, Entrust's self-depiction as a cybersecurity expert proved false. Contrary to its many representations and promises, Entrust utilized inadequate data security measures that it knew, or should have known, put the highly sensitive data entrusted to it at significant risk of

[1] https://www.entrust.com/company
[2] https://www.entrust.com/webinars
[3] https://en.wikipedia.org/wiki/Entrust

theft by or exposure to nefarious parties. Entrust, moreover, failed to meet the very cybersecurity standards that it underscored as critical for its clients' businesses.

6. In July 2022, due to Entrust's inadequate data security and failure to comply with federal and state data privacy standards, an unauthorized third party gained access to Entrust's digital environment (the "Data Breach"). Thereafter, the unauthorized third party gained access to and exfiltrated the files and records of numerous Entrust employees. However, Entrust, at least six months after the Data Breach, was continuing to disclose which of its employees were impacted.

7. With the sensitive files and records secured and stolen, the hackers purportedly issued a ransom demand to Entrust. However, Entrust has provided no public information on the ransom demand.

8. Plaintiff brings this class action against Entrust for its failure to secure and safeguard the confidential, personally identifiable information of its employees, also putting the data it holds on behalf of its customers at risk. The categories of stolen information about Entrust's current and former employees included names, employee identification numbers, contact information, Social Security numbers, bank account numbers, dates of birth ("Personally Identifying Information" or "PII"). The exfiltrated data also included some individuals' health information ("Private Health Information" or "PHI"). PII and PHI is collectively referred to as "Sensitive Information".

9. Due to Entrust's negligence, Plaintiff and the Class have suffered harm and are subject to a present and continuing risk of identity theft. Plaintiff's and the Class's Sensitive Information has been compromised and they must now undertake additional security measures to mitigate the damage caused by Entrust's actions.

10. Plaintiff Morrison is a former Entrust employee and Data Breach victim. Mr. Morrison worked for Entrust from approximately 2017 until 2022 and, as a condition of that employment, was required to provide his Sensitive Information to Entrust. Plaintiff reasonably believed that Entrust would take adequate steps to safeguard the Sensitive Information he entrusted to it. Defendant did not, resulting in the Data Breach.

11. The Data Breach impacted many of Entrust's clients and employees. The full scope of the Data Breach, however, is either not known or has not been publicly disclosed. In fact, Entrust appears to still be identifying which of its employees were affected by the Data Breach.

12. Plaintiff brings this Complaint on behalf of persons whose Sensitive Information was stolen during the Data Breach.

PARTIES

13. Plaintiff James Morrison is a resident of Belle Plaine, Minnesota. Mr. Morrison received a notice from Entrust in December 2022 that his Sensitive Information was exposed during Entrust's Data Breach. After the Data Breach, Mr. Morrison's PayPal account and Wells Fargo bank account experienced suspicious activity. Additionally, Mr. Morrison also experienced a noticeable increase in spam texts and phone calls after the Data Breach.

14. Entrust Corporation is a cybersecurity service provider incorporated in Delaware and headquartered in Minnesota, with its principal place of business located at 1187 Park Place Minneapolis, MN 55379.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and

costs, and there are more than 100 putative class members. Plaintiff and Entrust are citizens of different states. Class members and Entrust are also of different states.

16. 1This Court has jurisdiction over Entrust because it maintains its principal place of business in Minnesota, regularly conducts business in Minnesota, and has sufficient minimum contacts in Minnesota. Entrust intentionally availed itself of this jurisdiction by marketing and selling products and services from Minnesota to many businesses nationwide.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Entrust's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL BACKGROUND

a. Entrust

18. Entrust is a company located in Minneapolis, Minnesota, whose services include securing transactions, identifies, and data on behalf of companies and government entities. This includes managing and overseeing highly sensitive data.

19. Entrust also employs numerous Information Technology support specialists, analysts, and sales representatives at each of its offices. Plaintiff is a former employee of Entrust.

20. Entrust was founded in 1969 under the premise "that securing identities, transactions, and data has never been more important."[4] Entrust proclaims to be a global leader in the cybersecurity industry. As a provider of cybersecurity solutions that maintained PII, PHI, and other Sensitive Information, on behalf of their clients and employees, Entrust had a duty to safeguard the data provided by the organizations who were receiving or had received its services, as well as employees who were required to disclose their Sensitive Information by Entrust. Plaintiff

[4] https://youtu.be/FeCFO5rpeIc

and the Class had a reasonable expectation that the highly Sensitive Information provided to Entrust, and its clients impacted by the Data Breach, would be protected. Entrust, as the holder of that Sensitive Information, had an obligation to reasonably protect it against theft and misuse.

21. As detailed more fully below, Entrust failed to safely and securely store the Sensitive Information entrusted to it and failed to prevent it from being compromised during the Data Breach.

b. The Data Breach

22. Entrust claims to be the industry standard for secure transactions, identities, and data for businesses. As such, Entrust is well aware the business and government entities it services process some of the most valuable and targeted data for cybercriminals.

23. Entrust claims its cybersecurity services offer "security with a greater level of trust" through their data protection solutions, which purports to keep "enterprises, consumers, governments, citizens, and their data secure" through "high assurance security."[5]

24. Entrust also purports that it "continue[s] to acquire powerful brands, develop new technologies, and extend [its] global footprints" in order to "strengthen [its] position as a world leader in [its] industries" and "build trust into everything [it does]" so its clients had "the freedom to experience [their] world without compromise." [6]

25. Entrust's cybersecurity services are specialized for businesses who manage highly sensitive data. Entrust thus must oversee, manage, and protect its clients' and employees' sensitive data that includes personally identifying information (like names, addresses, and social security numbers), healthcare information (like medical records and histories), and financial information (like payroll data and banking account information).

[5] https://www.entrust.com/
[6] https://www.entrust.com/company/history

26. As both an employer and a cybersecurity company that handled highly sensitive aspects of its clients' businesses, Entrust understood the need to protect its employees' and clients' data and prioritize its data security. In fact, in 2014—long before Entrust's Data Breach—Entrust warned of the substantial costs of a data breach generally.[7]

27. Entrust explained that, in particular, "malware is emboldened by the green. It is not incidental that cybercriminals tend to target things like Social Security numbers and credit cards: these things present a means of accessing a person's identity. And once that identity is assumed, it can be exploited." Entrust further explains that "cybercrime black market may be more profitable than international drug crime."[8] As such, Entrust noted the valuable nature of Sensitive Information.

28. Entrust portrayed itself as a data security expert to its clients and the public. It provided a host of cybersecurity-related webinars and presentations to its clients, including "Securing Your Organization With A Credentials-Based Passwordless Solution," "Yes, You Can Have It All: How To Fight Financial Fraud And Delight Consumers At The Same Time," and "Protecting Digital Healthcare's Puppies And Unicorns."[9]

29. Entrust further represented that it was fully capable of securing its employees' and clients' highly sensitive data. As shown in Image 1 below, Entrust advertised that "The world's most entrusted organizations trust us."

[7] https://www.entrust.com/blog/2014/04/cybercrime-compromising-identity-reaping-profits-and-not-slowing-down-part-1/
[8] https://www.entrust.com/blog/2014/04/cybercrime-compromising-identity-reaping-profits-and-not-slowing-down-part-1/
[9] https://www.entrust.com/blog/?sfid=1060&sort_order=date+desc&_sft_category=cybersecurity-institute%2Cidentity-access-management&sf_paged=4

Image 1. Description of "The world's most Entrusted trust us."

30. Entrust also claimed it is "enables security with a greater level of trust, in every interaction and everywhere enterprises, people, and data move,"[10] as shown in Image 2 below.

31. *Image 2.* A picture of Entrust's advertisement related to its cybersecurity services.

[10] https://www.entrust.com/

32. Although Entrust's business involves providing cybersecurity services related to the storage and maintenance of highly sensitive data, it implemented inadequate data security practices that, as a purported cybersecurity expert, it knew or should have known, put its employees and clients at risk of having their sensitive data exposed.

33. As a condition of employment with Entrust, Defendant requires its employees to disclose Sensitive Information such as their names, Social Security numbers, and dates of birth.

34. On information and belief, Entrust collects and maintains employees' Sensitive Information in its computer systems.

35. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff would not have accepted the Defendant's employment offer, nor provided his Sensitive Information, to Entrust had he known that Entrust does not take all necessary precautions to secure the personal information given to it by its employees.

36. On June 18, 2022, Entrust was subjected to a ransomware attack that targeted Entrust's back-office system, which managed all of Entrust's client and employee data. Included in the ransomware attack was the Sensitive Information provided to Entrust it by its clients and employees.

37. The notorious LockBit ransomware gang claimed responsibility for the cyberattack, and went so far as creating a dedicated data leak page on which to publish the Sensitive Information stolen from Entrust.[11] In fact, LockBit began to release information obtained from the breach on the data leak page in August 2022 before the page was knocked offline.[12] LockBit is one of the

[11] https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-security-giant-entrust-leaks-data/
[12] https://siliconangle.com/2022/08/22/lockbit-ransomware-gang-knocked-offline-publishing-stolen-entrust-data/

most active ransomware actors, and Entrust, as a cybersecurity company, knew or should have known of the tactics that groups like LockBit employ.

38. As a cybersecurity service provider, Entrust had access to and controlled data from many, if not all, of its clients and employees. By breaching Entrust, the hackers gained access to Entrust's past and present clients' and employees' data that Entrust oversaw and managed.

39. In December 2022, Entrust began notifying its clients and employees of the Data Breach and that Sensitive Information may have been impacted.

40. For example, in its Notification Letter, Entrust reported "an unauthorized party accessed some of our back-office systems and may have acquired personal information." **Ex. A**[13] The cyber criminals launched a ransomware attack that obtained the Sensitive Information of Entrust's clients and. In response, Entrust reported it took measures to contain the threat, including retaining a data security expert and coordinating with law enforcement authorities. *Id*.

41. Through its Breach Notice, Entrust also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "take steps to help protect yourself." Ex. A.

42. Various notices have indicated the stolen Sensitive Information of Plaintiff and the Class included full names, dates of birth, bank account and routing numbers, Social Security numbers, driver's license numbers, employee's identification numbers, as well as health information.

43. However, the breach notice Entrust provided was unreasonably delayed. Many breach victims were not informed of the Data Breach until December 2022 although the breach "occurred on or around June 18, 2022." *Id.* Hundreds of thousands of Class members were notified

[13] A true and accurate copy of Entrust's Breach Notice is attached to this Complaint as Exhibit A.

even later. Plaintiff and the Class did not know to take action to secure their Sensitive Information and mitigate any associated risks or harm until six or more months after the breach occurred.

44. On information and belief, Defendant has offered complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that victims will face following the Data Breach. Indeed, the breach involves Sensitive Information that cannot be changed, such as Social Security numbers.

c. Data Breaches Lead to Identity Theft and Cognizable Injuries.

45. The personal, health, and financial information of Plaintiff and the Class, is valuable and has been commoditized in recent years.

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

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

48. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[14]

49. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement

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

has difficulty policing the "dark web" due to this encryption, which allows users and criminals to conceal identities and online activity.

50. Once Sensitive Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional Sensitive Information being harvested from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim.

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

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

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

54. Data breaches facilitate identity theft as hackers obtain victim's Sensitive Information and use it to siphon money from existing accounts, open new accounts in the names of their victims, or sell victims' Sensitive Information to others who do the same.

55. 46. Victims of identity theft often suffer indirect financial costs as well, including the costs incurred due to litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit.

56. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims

have to spend a considerable time repairing the damage caused by the theft of their Sensitive Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

57. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Sensitive Information. To protect themselves, Plaintiff and the Class (and the business entities whose information was breached) will need to be remain vigilant against unauthorized data use for years or even decades to come.

58. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new (and valuable) form of currency. In a FTC roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[15]

59. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[16]

60. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data

[15] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited September 22, 2021).
[16] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited February 12, 2023).

security into all business decision-making.[17] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry unapproved activity; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[18]

61. According to the FTC, unauthorized Sensitive Information disclosures wreak havoc on consumers' finances, credit history and reputation, and can take time, money and patience to resolve the fallout.[19] The FTC, as such, treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

62. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Entrust] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Entrust] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and

[17] Start With Security, A Guide for Business, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[18] *Id.*
[19] See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012), www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.

process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Entrust] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded Entrust's Data Breach, further clarify the measures businesses must take to meet their data security obligations.

63. Consumers place a high value on their PII and a greater value on their PHI, in addition to the privacy of their Sensitive Information. Research shows how much consumers value their data privacy, and the amount is considerable. Indeed, studies confirm that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US $30.49–44.62."[20]

64. By virtue of the Data Breach here and unauthorized release and disclosure of the Sensitive Information of Plaintiff and the Class, Entrust deprived Plaintiff and the Class of the substantial value of their Sensitive Information, to which they are entitled. As previously alleged, Entrust failed to provide reasonable and adequate data security, pursuant to and in compliance with industry standards and applicable law.

65. As a cybersecurity expert, Entrust was aware of the potential harm caused by a data breach. Entrust, as a company profiting from its cybersecurity services, understood better than

[20] See Il-Horn Hann et al., The Value of Online Information Privacy (Oct. 2002) available at http://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited September 22, 2021); see also Tsai, Cranor, Acquisti, and Egelman, The Effect of Online Privacy Information on Purchasing Behavior, 22 (2) Information Systems Research 254, 254 (June 2011).

most how important data security is and the ongoing nature of maintaining the latest technology and protocols for cyber security.

66. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen.

67. As a result, victims suffer immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

68. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial accounts and identity has been stolen. When Sensitive Information is stolen, accounts become less secure, and the information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

69. As a direct and proximate result of Entrust's wrongful actions and omissions here, Plaintiff and the Class have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*: (i) from the untimely and inadequate notification of the Data Breach, (ii) the resulting immediate and continuing risk of future ascertainable losses, economic damages and other actual injury and harm, (iii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are entitled to compensation; (iv) out-of-pocket expenses for securing identity theft protection and other similar necessary services; (v) the diminution in value of their Sensitive Information; (vi) the compromise and continuing publication of their Sensitive Information; (vii) unauthorized use of stolen Sensitive Information; and (viii) the continued risk

to their Sensitive Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Sensitive Information in their possession.

d. Defendant Failed to Adhere to FTC Guidelines

70. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Sensitive Information.

71. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

72. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

73. The FTC recommends that companies not maintain information 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.

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

75. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' Sensitive Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

e. Defendant Violated HIPAA

76. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' 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.[21]

77. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[22]

78. 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:

[21] 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.

[22] *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).

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 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).

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

Plaintiff's Experience

80. Plaintiff James Morrison is a former employee of Defendant—and thus he was injured by Defendant's Data Breach. Plaintiff was employed by Entrust from approximately 2017 until July 2022.

81. As a condition of his employment, Plaintiff was required to provide his Sensitive Information to Defendant. Plaintiff provided his Sensitive Information to Entrust and trusted that the company would use reasonable measures to protect it given its position as a cybersecurity industry leader, its internal policies and representations, and state and federal law.

82. Entrust deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for months.

83. As a direct and proximate result of Entrust's wrongful actions or omissions, Plaintiff Morrison received a Notice that his Sensitive Information—on Entrust's systems—was also included in the batch of information stolen during the Data Breach. Entrust was Plaintiff Morrison's former employer.

84. After the Data Breach, Mr. Morrison's PayPal account and Wells Fargo bank account experienced suspicious activity. Mr. Morrison was forced to spend time reviewing his banking statements to identify any fraudulent transactions.

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

86. Plaintiff now faces an ongoing, substantial risk of suffering identity theft and fraud in the future, as he has *already* suffered identity theft multiple times and because the breach involved information he cannot change, like his Social Security number. As a result, Plaintiff has spent considerable time and effort monitoring his accounts to protect himself from further identity theft. Plaintiff fears for his personal financial security and uncertainty over what information was revealed in the Data Breach.

87. Mr. Morrison has suffered actual injury in the form of damages to and diminution in the value of his Sensitive Information—a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

88. Mr. Morrison has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Sensitive Information being placed in the hands of unauthorized third parties and criminals.

89. Mr. Morrison has a continuing interest in ensuring that his Sensitive Information, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

CLASS DEFINITION AND ALLEGATIONS

90. Plaintiff brings this class action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following class:

91. All individuals residing in the United States whose Sensitive Information was compromised in the Data Breach disclosed by Entrust in July 2022.

92. Excluded from the Class are Entrust, their agents, affiliates, parents, subsidiaries, any entity in which Entrust has a controlling interest, any Entrust officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

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

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

a. **Numerosity**. The members of the Class are so numerous that joinder of all members of the Class is impracticable.

b. **Commonality and Predominance**. Plaintiff and the Class's claims raise predominantly common fact and legal questions, which predominate over any questions affecting individual Class members, that a class wide proceeding can answer for all Class members. Indeed, it will be necessary to answer the following questions:

    a. Whether Entrust had a duty to use reasonable care in safeguarding Plaintiff and the Class's Sensitive Information;

    b. Whether Entrust 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 Entrust was negligent in maintaining, protecting, and securing Plaintiff and the Class's Sensitive Information;

d. Whether Entrust breached contract promises to safeguard Plaintiff and the Class's Sensitive Information;

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

f. Whether Entrust's Breach Notice was reasonable;

g. Whether the Data Breach caused Plaintiff and the Class's injuries;

h. What the proper damages measure is; and

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

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

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class members' interests. He has also retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that would be entailed by individual litigation of their claims against Entrusts. It would thus be virtually impossible for the Class members, on an individual basis, to

obtain effective redress for the wrongs done to them. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts and would also increase the delay and expense to all parties and the courts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances here.

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

95. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

96. Entrust owed to Plaintiff and the Class a duty of reasonable care to protect Plaintiff's and the Class's data from the foreseeable threat of theft during a Data Breach. This duty arose from several sources.

97. Plaintiff and members of the Class entrusted their Sensitive Information to Entrust. Defendant owed a duty to Plaintiff and the Class to exercise reasonable care in safeguarding and protecting their personal data and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties. This duty included, among other things, designing, maintaining, and testing Defendant's security systems to ensure the personal data of Plaintiff's and the Class was adequately secured and protected, including using encryption technologies. Defendant further had a duty to implement processes that would detect a breach of its security system in a timely manner.

98. Entrust was under a basic duty to act with reasonable care when it undertook to collect, create, and store Plaintiff's and the Class's sensitive data on its computer system, fully aware–as any reasonable entity of its size would be–of the prevalence of data breaches and the resulting harm such a breach would cause. The recognition of Defendant's duty to act reasonably in this context is consistent with, *inter alia*, the Restatement (Second) of Torts § 302B (1965), which recounts a basic principle: an act or omission may be negligent if the actor realizes or should realize it involves an unreasonable risk of harm to another, even if the harm occurs through the criminal acts of a third party.

99. Entrust also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiff and the Class can take appropriate measures to avoid unauthorized use of their Sensitive Information, accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Entrust's unreasonable misconduct.

100. Defendant knew that the personal data of Plaintiff and the Class was personal and sensitive information that is valuable to identity thieves and other criminals. Defendant also knew of the serious harms that could happen if the personal data of Plaintiff and the Class was wrongfully disclosed, that disclosure was not fixed.

101. By being entrusted by Plaintiff and the Class to safeguard their personal data, Defendant had a special relationship with Plaintiff and the Class. Plaintiff and the Class agreed to provide their personal data with the understanding that Defendant would take appropriate measures

to protect it and would inform Plaintiff and the Class of any security concerns that might call for action by Plaintiff and the Class.

102. Entrust breached its duty to Plaintiff and the Class by failing to implement and maintain reasonable security controls that were capable of adequately protecting the Sensitive Information of Plaintiff and the Class.

103. Entrust also breached its duty to timely and accurately disclose to its clients and employees, Plaintiff and the Class, that their Sensitive Information had been or was reasonably believed to have been improperly accessed or stolen.

104. Entrust's negligence in failing to maintain reasonable data security is further evinced by its failure to comply with legal obligations and industry standards, and the delay between the date of the Data Breach and the time when Entrust disclosed it.

105. The injuries to Plaintiff and the Class were reasonably foreseeable to Entrust because laws and statutes, and industry standards require it to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiff's and the Class's Sensitive Information.

106. The injuries to Plaintiff and the Class were reasonably foreseeable because Entrust knew or should have known that systems used for safeguarding Sensitive Information were inadequately secured and exposed consumer Sensitive Information to being breached, accessed, and stolen by hackers and unauthorized third parties. As such, Entrust's own misconduct created a foreseeable risk of harm to Plaintiff and the Class.

107. Entrust implemented knowingly deficient data security measures and failed to adopt reasonable measure that could protect the Sensitive Information of Plaintiff and the Class, and those deficient security measures proximately caused Plaintiff's and the Class's injuries

because they directly allowed hackers to easily access Plaintiff and the Class's Sensitive Information. This ease of access allowed the hackers to steal Sensitive Information of Plaintiff and the Class, which could lead to dissemination in black markets.

108. As a direct proximate result of Entrust's conduct, Plaintiff and the Class have suffered theft of their Sensitive Information. Entrust allowed thieves access to Plaintiff's and the Class's Sensitive Information, thereby decreasing the security of Plaintiff's and the Class's financial and health accounts, making Plaintiff's and the Class's identities less secure and reliable, and subjecting Plaintiff and the Class to the imminent threat of identity theft. Not only will Plaintiff and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

109. Entrust's conduct warrants moral blame because it actively solicited its services to its clients, wherein it used, handled and stored the Sensitive Information of Plaintiff and the Class without disclosing that its security was inadequate. Holding Entrust accountable for its negligence will further the policies embodied in the law by incentivizing cybersecurity service providers to properly secure sensitive consumer information and protect the consumers who rely on these companies every day.

SECOND CAUSE OF ACTION
Negligence Per Se
(On Behalf of Plaintiff and the Class)

110. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

111. Entrust's unreasonable data security measures and failure to timely notify Plaintiff and the Class of the Data Breach violates Section 5 of the FTC Act. Although the FTC Act does

not create a private right of action, it requires businesses to institute reasonable data security measures and breach notification procedures, which Entrust failed to do.

112. Section 5 of the FTCA, 15 U.S.C. § 45, prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice of businesses like Entrust failing to use reasonable measures to protect sensitive health and financial data. The FTC publications and orders described above also form the basis of Entrust's duty.

113. Entrust violated Section 5 of the FTC Act by failing to use reasonable measures to protect sensitive health and financial data and by not complying with applicable industry standards. Entrust's conduct was particularly unreasonable given the highly sensitive nature and amount of data it stored and the foreseeable consequences of a Data Breach should Entrust employ unreasonable, inadequate data security.

114. Entrust's violation of Section 5 of the FTC Act constitutes negligence per se.

115. Plaintiff and the Class are within the class of persons Section 5 of the FTCA (and similar state statutes) were intended to protect. Additionally, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by Plaintiff and the Class.

116. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class Members' PHI.

117. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed supra. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that

Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

118. As a direct and proximate result of Entrust's negligence per se, Plaintiff and the Class have suffered and continue to suffer injury.

THIRD CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

119. Plaintiff incorporates by reference all previous allegations as though fully set forth herein.

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

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

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

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

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

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

123. The Court should also issue corresponding injunctive relief requiring Entrust to employ adequate security protocols consistent with industry standards to protect its clients' (i.e., Plaintiff's and the Class's) data.

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

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

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

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

127. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

128. Entrust offered to employ Plaintiff and members of the Class in exchange for their Sensitive Information.

129. Plaintiff and the Class entrusted their Sensitive Information to Defendant at the time they entered into an employment relationship with Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed, based on its representations and actions to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

130. Entrust agreed they would not disclose the Sensitive Information it collects to unauthorized persons. Entrust also promised to safeguard Sensitive Information.

131. Plaintiff and the Class accepted Entrust's offers by disclosing their Sensitive Information to Entrust in exchange for employment with Entrust.

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

133. Implicit in the parties' agreement was that Entrust would provide Plaintiff and the Class with prompt and adequate notice of all unauthorized access and/or theft of their Sensitive Information.

134. Plaintiff and the Class would not have entrusted their Sensitive Information to Entrust in the absence of such agreement with Entrust.

135. Entrust materially breached the contract(s) it had entered with Plaintiff and the Class by failing to safeguard such information and failing to notify them promptly of the Data Breach that compromised such information. Entrust further breached the implied contracts with Plaintiff and the Class by:

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

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

c. Failing to ensure the confidentiality and integrity of Sensitive Information that Entrust created, received, maintained, and transmitted.

136. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Entrust's material breaches of their agreement(s).

137. Plaintiff and the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Entrust.

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

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

140. Entrust failed to advise Plaintiff and the Class of the Data Breach promptly and sufficiently.

141. In these and other ways, Entrust violated its duty of good faith and fair dealing.

142. Plaintiff and the Class have sustained damages because of Entrust's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

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

143. Plaintiff and the Class incorporate the above allegations as if fully set forth herein.

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

145. Plaintiff and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Sensitive Information. They also conferred a benefit on Defendant by providing their employment services.

146. Entrust appreciated or had knowledge of the benefits conferred upon them by Plaintiff and the Class. Entrust also benefited from the receipt of Plaintiff's and members of the Class's Sensitive Information, as this was used to provide its goods and services.

147. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Sensitive Information and by retaining the benefit of Plaintiff's and the Class's labor.

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

149. Under principals of equity and good conscience, Entrust should not be permitted to retain the full value of Plaintiff and the d Class's services and their Sensitive Information because Entrust failed to adequately protect their Sensitive Information. Plaintiff and the d Class would not have provided their Sensitive Information to Entrust had they known Entrust would not adequately protect their Sensitive Information.

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests that the Court enter an order:

a. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

b. Finding that Defendants engaged in the unlawful conduct as alleged herein;

c. Enjoining Defendants' conduct and requiring Defendants to implement proper data security practices, specifically:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the Sensitive Information of Plaintiff and the Class unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and the Class's Sensitive Information;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling Sensitive Information, as well as protecting the Sensitive Information of Plaintiff and the Class;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting Sensitive Information;

xiv. requiring Defendants implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential Sensitive Information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers;

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class and Subclasses, and to report any deficiencies with compliance of the Court's final judgment;

xviii. requiring Defendants to design, maintain, and test its computer systems to ensure that Sensitive Information in its possession is adequately secured and protected;

xix. requiring Defendants to disclose any future data breaches in a timely and accurate manner;

xx. requiring Defendants to implement multi-factor authentication requirements;

xxi. requiring Defendants' employees to change their passwords on a timely and regular basis, consistent with best practices; and

xxii. requiring Defendants to provide lifetime credit monitoring and identity theft repair services to Class members.

a. Awarding Plaintiff and the Class damages;

b. Awarding Plaintiff and Class pre-judgment and post-judgment interest on all amounts awarded;

c. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses; and

d. Granting such other relief as the Court deems just and proper.

JURY TRIAL DEMANDED

151. Plaintiff and the Class demand a trial by jury on all issues so triable.

Dated: February 17, 2023

TURKE & STRAUSS LLP

By: */s/ Raina C. Borrelli*

Raina C. Borrelli
raina@turkestrauss.com
Samuel J. Strauss (*pro hac vice*)
sam@turkestrauss.com
Brittany Resch
brittanyr@turkestrauss.com
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775
Facsimile: (608) 509-4423

Attorneys for Plaintiff and Proposed Class

ClassAction.org
