UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

MARY DELL PAYNE, individually and on behalf of all others similarly situated, Plaintiff, vs. SARATOGA HARNESS RACING, INC., and SARATOGA CASINO HOLDINGS LLC, Defendants.	Case No. 1:25-cv-614 (AMN/DJS) **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Mary Dell Payne ("Plaintiff") brings this Class Action Complaint against Defendants Saratoga Harness Racing, Inc. ("SHR"), and Saratoga Casino Holdings LLC ("SCH") (collectively, "Defendants"), on behalf of herself and all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Based in Saratoga Springs, New York, Defendant Saratoga Harness Racing, Inc. is a privately held gaming and racing company founded in 1941, originally operating the Saratoga Raceway, one of the nation's first pari-mutuel harness tracks. Over the years, the company has expanded beyond racing to include gaming and hospitality services. To manage and grow its portfolio, SHR established Saratoga Casino Holdings LLC, a wholly owned subsidiary that oversees the company's gaming and entertainment properties. Now operating under SCH, SHR's

business includes casinos, live harness racing, video lottery terminals, electronic table games, hotel accommodations, dining, and simulcast wagering.[1]

2. SCH owns and operates several venues, including Magnolia Bluffs Casino Hotel in Mississippi, which Plaintiff had visited occasionally prior to receiving a notice of data breach from SHR.[2]

3. On or about December 30, 2024, SHR notified the Office of the Attorney General of Maine, along with some of the impacted consumers, about a significant data breach that occurred between October 31 and November 1, 2024.[3] SHR updated its notice to the Maine Attorney General's Office subsequently, including on January 31, 2025, and most recently on April 3, 2025.[4]

4. According to SHR's notice, on November 1, 2024, SHR experienced a network disruption. Its subsequent investigation confirmed that between October 31 and November 1, 2024, an unknown and unauthorized individual or individuals accessed SHR's internal network and exfiltrated certain sensitive and confidential personal information of approximately 9,527 consumers, including Plaintiff and Class Members (the "Data Breach").[5] The sensitive personally identifiable information ("PII") stolen by cybercriminals in the Data Breach includes but is not

---

[1] *See* https://saratogacasino.com/ (last visited May 12, 2025).

[2] *See* https://saratogacasino.com/saratoga-casino-holdings-llc-marks-one-year-since-acquisition-of-magnolia-bluffs-casino-hotel/?utm_source=chatgpt.com (last visited May 12, 2025).

[3] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8e662a53-d105-4ab4-b521-bfd6b3e74852.html; and https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/986115fe-cee4-44c9-b7c0-ae818b977e12.html (last visited May 12, 2025).

[4] *See* Sample Notice of Data Breach available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/34543f35-860e-45a8-b59d-8026b2a8c40e.html (last visited May 12, 2025).

[5] *Id*.

limited to, Plaintiff's and Class Members' first and last names, Social Security numbers, and driver's license or other state ID numbers (collectively, "PII" or "Private Information").[6]

5. In addition to the theft of her Private Information, Plaintiff experienced unauthorized transactions totaling $756 on her Cash App account. Following the Data Breach, she was also targeted by scam attempts and inundated with unsolicited spam communications. These events demonstrate that the breach was successful, that hackers accessed confidential information, and that the unredacted, stolen Private Information was likely offered for sale to other criminals. As a result of Defendants' failure to secure their internal systems, Plaintiff's and Class Members' Private Information remains exposed and vulnerable to malicious use.

6. Plaintiff's Private Information was compromised as a result of Defendants' negligent and careless acts, omissions, and overall failure to safeguard customer data.

7. In addition to failing to prevent the Data Breach, Defendants also failed to detect and stop it while cybercriminals maintained access to their internal systems for two consecutive days between October 31 and November 1, 2024.

8. Moreover, Defendants failed to notify customers or any state Attorneys General about the Data Breach until December 30, 2024—nearly two months after discovering it on November 1, 2024. Some affected individuals, including Plaintiff, did not receive any notification until approximately April 3, 2025—more than five months after the initial discovery.

9. Upon information and belief, the stolen Private Information of the approximately 9,527 individuals affected by the Data Breach holds significant value to cybercriminals.

10. Plaintiff brings this class action lawsuit on behalf of herself and all others similarly situated to address Defendants' failure to adequately safeguard the Private Information

[6] *Id*.

they collected and maintained, as well as their failure to provide timely and sufficient notice to Plaintiff and other Class Members regarding the unauthorized access by an unknown third party and the specific types of information that were compromised.

11. Plaintiff and Class Members, as customers of Defendants, have suffered injury as a result of Defendants' negligent conduct. These injuries include, but are not limited to:(i) the loss or diminution in value of their Private Information; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, credit card fraud, and/or unauthorized use of their Private Information; (iii) lost opportunity costs and time spent attempting to mitigate the consequences of the Data Breach; and (iv) the ongoing and significantly increased risk to their Private Information, which (a) remains available on the Dark Web or otherwise publicly accessible for malicious use, and (b) remains in Defendants' possession and is vulnerable to further unauthorized disclosures as long as Defendants fail to implement adequate and appropriate data protection measures.

II. PARTIES

12. Plaintiff Mary Dell Payne is a resident and citizen of Port Gibson, Mississippi, where she intends to remain. She received a Notice of the Data Breach from SHR, dated April 3, 2025, on or about that date.

13. Defendant Saratoga Harness Racing, Inc. is a New York Domestic Business Corporation with its principal place of business within Saratoga County in New York. Its principal place of business is located at 342 Jefferson Street, Saratoga Springs, New York 12866. It is the sole member of Saratoga Casino Holdings LLC.

14. Defendant Saratoga Casino Holdings LLC is a New York State limited liability company doing business within Saratoga County in New York. Its principal place of business is also located at 342 Jefferson Street, Saratoga Springs, New York, 12866.

III. JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants. Moreover, Plaintiff Payne is a citizen of Mississippi and therefore diverse from Defendants, which are headquartered and incorporated in New York.

16. This Court has personal jurisdiction over Defendants because they are headquartered and incorporated in New York and conduct business in the state.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District.

IV. FACTUAL ALLEGATIONS

Background

18. Defendant Saratoga Harness Racing, Inc. is a privately held gaming and hospitality company headquartered in Saratoga Springs, New York. Founded in 1941 with the establishment of Saratoga Raceway—one of the nation's earliest pari-mutuel harness racing tracks—the company has expanded its operations through its holding entity, Saratoga Casino Holdings LLC. SCH owns and operates several venues, including Saratoga Casino Hotel in New York, Saratoga Casino Black Hawk in Colorado, and Magnolia Bluffs Casino Hotel in Mississippi. SHR's current portfolio includes gaming services such as slot machines, video lottery terminals, and electronic table games, along with live harness racing, hotel accommodations, dining, and simulcast wagering.

19. As part of their business practices, Defendants collect and maintain the Private

Information of their customers, such as Plaintiff and Class Members, including but not limited to their names, Social Security numbers, driver's license information, and/or state ID numbers.

20. In order to receive services from Defendants, it was mandatory for Plaintiff and Class Members to submit their Private Information.

21. Upon information and belief, Defendants store customers' Private Information within their computer networks for extended periods of time, as evidenced by the hackers' ability to access and steal the sensitive Private Information of approximately 9,527 current and former customers during the Data Breach.

22. According to Defendants' Privacy Policy, Defendants represent that they "do not sell or disclose information that identifies our users personally or makes it possible for other parties to contact them directly without our users' consent."[7]

23. However, Defendants have clearly failed to uphold their promise or implement reasonable security measures to protect Plaintiff's and Class Members' Private Information.

24. As a sophisticated business that collects and retains large volumes of sensitive and confidential Private Information from consumers, Defendants knew or should have known that it was an obvious target for cybercriminals, and that robust cybersecurity measures were therefore critically important.

25. Had Plaintiff and Class Members known about Defendants' lax cybersecurity practices, they would not have entrusted their Private Information to Defendants' system.

26. The stolen sensitive Private Information is all that hackers would need to commit fraudulent and criminal acts against the individuals affected by the Data Breach.

///

[7] *See* https://saratogacasino.com/privacy-policy/(last visited May 12, 2025).

The Data Breach

27. On or about December 30, 2025, SHR notified the Maine Attorney General's Office about the Data Breach about a significant cybersecurity incident that occurred between October 31 and November 1, 2024.[8] SHR updated its notice to the Attorney General's Office in Maine subsequently on January 31, 2025, and most recently on April 3, 2025. [9]

28. On or about April 3, 2025, Defendants sent Plaintiff and Class Members an untitled Notice of Data Breach (the "Notice").[10] In the Notice, Defendants notified the recipients that:

> **What Happened?** On November 1, 2024, we experienced a network disruption that limited our ability to access certain files and systems on our network. We immediately began an investigation with the assistance of third-party specialists to determine the full nature and scope of the incident. The investigation determined that an unknown party potentially accessed some files on our network without authorization between October 31 and November 1, 2024. Therefore, we initiated a thorough review of the files at issue to determine the type of information they contained and to whom the information related.
>
> **What Information Was Involved?** This review is now complete and has determined that the files at issue include your name in combination with Social Security number and driver's license or State ID number.[11]

29. Notably, the Notice sent to affected individuals also states that "[w]e have no reason to believe any of the information concerning you described above has been or will be

---

[8] *See* Sample of the Notice of Data Breach available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be28792a1252b4f8318/34543f35-860e-45a8-b59d-8026b2a8c40e.html (last visited May 12, 2025).

[9] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/986115fe-cee4-44c9-b7c0-ae818b977e12.html; and https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/34543f35-860e-45a8-b59d-8026b2a8c40e.html (last visited May 12, 2025).

[10] *See* Sample of the Notice of Data Breach available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/34543f35-860e-45a8-b59d-8026b2a8c40e.html (last visited May 12, 2025).

[11] *Id*.

misused."[12] This reassurance, however, stands in stark contrast to the reality of the Data Breach. The Notice not only downplays the seriousness of the incident but also lulls affected individuals into a false sense of security, rather than equipping them with the urgency and information necessary to protect themselves.

30. While cybercriminals maintained access to Defendants' systems for two consecutive days - October 31 and November 1, 2024 - Defendants failed to detect or stop the ongoing intrusion. This failure highlights Defendants' lack of adequate cybersecurity safeguards, as well as their noncompliance with industry standards and insufficient sensitivity to the risks associated with storing consumers' Private Information.

31. To make matters worse, although the Data Breach was discovered on November 1, 2024, Defendants did not notify any Attorneys General or affected consumers until December 30, 2024, nearly two months later. Many consumers, including Plaintiff, did not become aware of the breach until as late as April 3, 2025, five full months after the initial discovery. This extended delay deprived victims of the opportunity to promptly mitigate harm, such as by monitoring their accounts, freezing credit, or taking other protective measures.

32. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiff and Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

[12] *Id*.

34. Had Plaintiff and Class Members known of Defendants' deficient cybersecurity practices, they would not have submitted their most sensitive and confidential personal information.

The Data Breach was Foreseeable

35. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the hospitality services industry preceding the date of the Data Breach.

36. In 2022, there were 1,802 data breaches, nearly eclipsing 2021's record, wherein 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[13] The 330 reported breaches in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[14]

37. According to Bluefin, "[t]he restaurant and hospitality industries have been hit particularly hard by data breaches, with hotel brands, restaurants and establishments targeted by hackers in 2019."[15]

38. Another report says that the "companies in the food and beverage industry are the most at risk from cybercriminals."[16]

---

[13] *See* "*2021 Data Breach Annual Report*" (ITRC, Jan. 2022) *available at* https://notified.idtheftcenter.org/s/, at 6 (last visited May 12, 2025).

[14] *See* "*Data Breaches Hit Lots More People in 2022*" (Jan. 25, 2023) *available at* https://www.cnet.com/tech/services-and-software/data-breaches-hit-lots-more-people-in-2022/ (last visited May 12, 2025).

[15] https://www.bluefin.com/bluefin-news/the-rise-in-restaurant-data-breaches-and-the-need-to-devalue-consumer-data/ (last visited May 12, 2025).

[16] https://www.industryweek.com/finance/article/21959093/food-and-beverage-industry-most-at-risk-for-cyber-attack (last visited May 12, 2025).

39. According to Kroll, "data-breach notifications in the food and beverage industry shot up 1,300% in 2020."[17]

40. Furthermore, in light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

41. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

42. Despite the prevalence of public announcements of data breaches and data security compromises, and despite their own acknowledgment of their duties to keep Private Information confidential and secure, Defendants failed to take appropriate steps to protect the Private Information of Plaintiff and the Class from being compromised.

43. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard their computer systems, networks, and data. Defendants' 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 and cyber-attacks;

[17] https://www.darkreading.com/attacks-breaches/data-breaches-surge-in-food-and-beverage-other-industries/d/d-id/1341336 (last visited May 12, 2025).

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions, encryptions, brute-force attempts, and clearing of event logs;

d. Failing to apply all available security updates;

e. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

f. Failing to practice the principle of least-privilege and maintain credential hygiene;

g. Failing to avoid the use of domain-wide, admin-level service accounts;

h. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords, and;

i. Failing to properly train and supervise employees in the proper handling of inbound emails.

44. As a result of outdated computer systems in need of critical security upgrades and inadequate procedures for addressing cybersecurity threats, Defendants negligently and unlawfully failed to safeguard the Private Information of Plaintiff and Class Members.

45. Accordingly, as outlined below, Plaintiff and Class Members now face a substantial, increased, and present risk of fraud and identity theft.

46. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendants because of their inadequate data security practices, for which they gave good and valuable consideration.

Defendants Fails to Comply with FTC Guidelines

47. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that 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.

48. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer 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. 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.

49. The FTC further recommends that companies not maintain 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 suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

50. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, 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.

51. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to

customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

52. Defendants were at all times fully aware of their obligation to protect the Private Information of customers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

53. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices.

54. Best cybersecurity practices that are standard in Defendants' industry 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; training staff regarding critical points.

55. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity 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 established standards in reasonable cybersecurity readiness.

56. These foregoing frameworks exist and applicable to industry standards in Defendants' industry. Defendants knew it was a target for hackers. Despite understanding the risks and consequences of inadequate data security, Defendants failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

Value of Personally Identifiable Information

57. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[18] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[19] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

58. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[20] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who, in turn, aggregates the information and provides it to marketers or app developers.[21] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[22]

59. As a result of the Data Breach, Plaintiff's, and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any

---

[18] *See* Anita George, "*Your personal data is for sale on the dark web. Here's how much it costs*," DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited May 12, 2025).

[19] *See* Brian Stack, "*Here's How Much Your Private Information Is Selling for on the Dark Web*," EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited May 12, 2025).

[20] *See* David Lazarus, "*Column: Shadowy data brokers make the most of their invisibility cloak*," LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited May 12, 2025).

[21] *See* Data Coup, https://datacoup.com/ (last visited May 12, 2025).

[22] *See "Frequently Asked Questions*," Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited November 27, 2023).

consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is likely readily available to others, and the rarity of the Private Information has been destroyed, thereby causing additional loss of value.

60. The fraudulent activity resulting from the Data Breach may not come to light for years, and Plaintiff and Class Members face a risk of fraud and identity theft as a result of the Data Breach.

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

61. Defendants were well aware that the Private Information they collect is highly sensitive, and of significant value to those who would use it for wrongful purposes, like the operators who perpetrated this cyber-attack.

62. 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."[23]

63. 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.

64. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is

[23] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited on May 12, 2025) ("GAO Report").

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.

65. For example, armed with just a name and date of birth, a data thief can use 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.

66. 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.

67. 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 (consider an extended fraud alert that lasts for 7 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.[24]

68. 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.

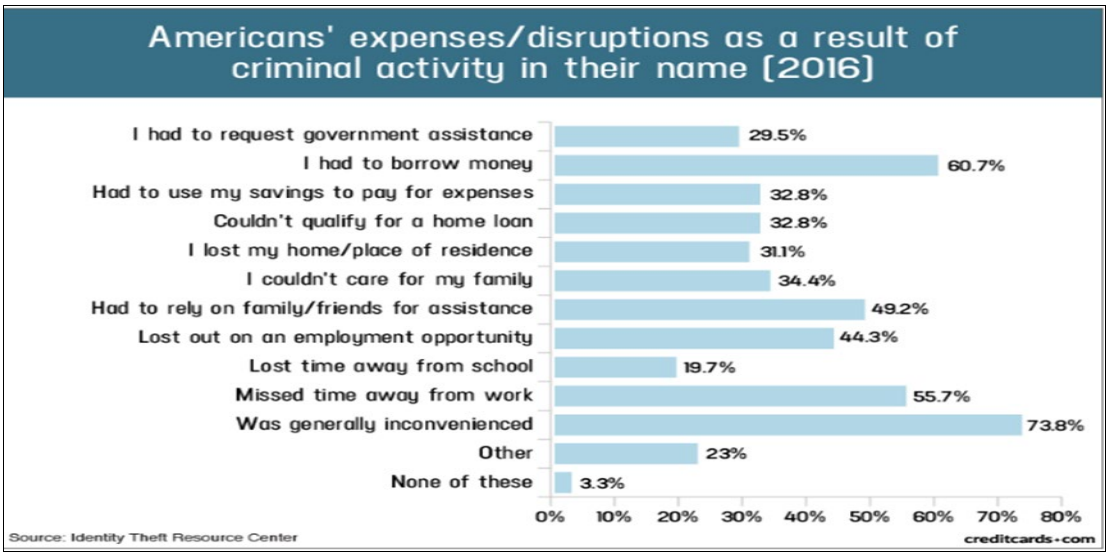
69. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

70. 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

[24] *See* https://www.identitytheft.gov/Steps (last visited on May 13, 2025).

victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

71. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[25]



72. Plaintiff and Class Members have experienced one or more of these harms as a result of the Data Breach.

73. Furthermore, theft of Private Information is also gravely serious. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

74. Moreover, there may be a time lag between when harm occurs versus when it is

[25] *See* Jason Steele, *Credit Card Fraud and ID Theft Statistics,* CREDITCARDS.COM (June 11, 2021), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited May 12, 2025) [https://web.archive.org/web/20200918073034/, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/].

discovered, and also between when Private Information is stolen and when it is used. 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 has 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.[26]

75. 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.

76. There is a strong probability that entire batches of stolen payment card information have been dumped or are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

77. Plaintiff and Class Members have suffered and will continue to suffer injuries as a direct result of the Data Breach, including substantial time and expense relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Removing withdrawal and purchase limits on compromised accounts;

[26] *See* U.S. Gov't Accountability Off., GAO 07737, "*Private Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*," at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last visited November 27, 2023).

f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Resetting automatic billing instructions; and

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

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

79. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

80. As a direct and proximate result of the Data Breach, Plaintiff's Private Information was exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiff and Class Members.

81. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an immediate and continuing increased risk of harm from fraud. Plaintiff and Class Members now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing, or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

82. Plaintiff 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.

83. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in similar cases.

84. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiff and Defendants included Defendants' contractual obligation to provide adequate data security, which Defendants failed to provide. Thus, Plaintiff and Class Members did not get what they paid for.

85. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial accounts and records for misuse.

86. Plaintiff and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property, including Private Information;

b. Improper disclosure of their Private Information;

c. The present and continuing injury flowing from potential fraud and identity theft posed by customers' Private Information being placed in the hands of criminals;

d. Damages flowing from Defendants' untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. 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;

g. Ascertainable losses in the form of deprivation of the value of customers'

Private Information for which there is a well-established and quantifiable national and international market; and,

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

87. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, particularly given the sensitive nature of their purchases, and of the foreseeable consequences that would occur if Defendants' data security system was breached (as it had been as recently as 2020), including, specifically, the significant costs and risks that would be imposed on Plaintiff and Class Members as a result of a breach.

88. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

89. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on Defendants' storage platform, amounting to numerous individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

90. While SHR has offered 12 months of complimentary credit monitoring or identity theft protection services, such measures are inadequate to safeguard Plaintiff and Class Members from the long-term risks they now face. Given the sensitive nature of the Private Information involved, including data that cannot be changed or easily replaced, the harm and exposure resulting from the Data Breach will persist well beyond the limited duration of the services provided.

91. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures, and failure to protect the Private Information of Plaintiff and Class Members.

92. Moreover, substantial delay in providing notice of the Data Breach deprived Plaintiff and Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendants' delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members was and has been driven even higher.

Plaintiff Mary Dell Payne's Experience

93. Plaintiff Mary Dell Payne ("Plaintiff Payne") has been a loyal customer at Magnolia Bluffs Casino Hotel, owned and operated by SCH in Natchez, Mississippi.

94. Upon visiting Defendants' casino, Plaintiff Payne was required to provide Defendants with her Private Information, including but not limited to her full name, Social Security number, driver's license information, and/or other government-issued ID information.

95. On or about April 3, 2025, Plaintiff Payne received the Notice from SHR indicating that her Private Information had been improperly accessed and exfiltrated during a cybersecurity incident that was detected by SHR on or about November 1, 2024.

96. As a result of the Data Breach, Plaintiff Payne has experienced a significant increase in spam communications, including unsolicited emails, phone calls, and text messages. The volume of spam became so overwhelming that she was forced to change her phone number.

97. Moreover, some of the unsolicited spam falsely claimed to be from debt collectors and included threats to visit her home to collect money, despite having no legitimate connection to Plaintiff Payne, causing additional distress and concern for her safety.

98. Additionally, Plaintiff Payne suffered actual injury from having her Private Information compromised and/or stolen as a result of the Data Breach.

99. In or around January 2025, Plaintiff Payne suffered out-of-pocket and unreimbursed financial losses of approximately $756 through her Cash App, as a direct result of fraud stemming from the Data Breach. She also sustained damage to, and a diminution in the value of, her Private Information - a form of intangible property that Plaintiff entrusted to Defendants for the purpose of receiving services at their casino and which was compromised as a result of the Data Breach.

100. Furthermore, in or around April 2025, an unknown party attempted to scam Plaintiff for $3,000 through email. Although the attempt was ultimately unsuccessful, it caused Plaintiff Payne significant stress and required considerable time and effort to address and mitigate the attempted fraud.

101. Following the Data Breach, Plaintiff has also noticed fluctuations in her credit score, which may be indicative of unauthorized activities.

102. Plaintiff Payne made reasonable efforts to mitigate the impact of the Data Breach since she received the Notice, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; actively checking her credit monitoring service; blocking unsolicited spam communications; changing her phone number; and consulting legal counsel for her rights. Plaintiff Payne has already spent at least 6 hours dealing with the Data Breach—valuable time that she otherwise would have spent on other activities, including recreation.

103. As a result of the Data Breach, Plaintiff Payne has suffered anxiety as a result 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

her Private Information for purposes of identity crimes, fraud, and theft. Plaintiff Payne is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

104. Plaintiff Payne suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by Private Information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

105. Plaintiff Payne has a continuing interest in ensuring that her Private Information, which remains in possession of Defendants, is protected and safeguarded from future breaches.

106. Plaintiff Payne suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her Private Information, a form of property that Defendants obtained from Plaintiff Payne; (b) violation of her privacy rights; (c) actual unreimbursed financial losses as a direct result of the Data Breach; (d) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

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

Impact on the Class

108. Simply put, Plaintiff and Class Members now face a 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.

109. Plaintiff and Class Members have been and face a substantial risk of being targeted in the future, subjected to phishing, data intrusion, and other illegal actions based on their Private Information as potential fraudsters could use that information to target such schemes more effectively.

110. Plaintiff and Class Members will need identity theft protection services and credit monitoring services for their respective lifetimes, considering the immutable nature of the Private Information at issue, especially their Social Security numbers.

111. Plaintiff 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 cyber-attack.

112. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the cyber-attack. Numerous courts have recognized the propriety of loss of value damages in related cases.

113. Class Members were also damaged via benefit-of-the-bargain damages, in that they overpaid for a service that was intended to be accompanied by adequate data security but was not. Part of the price Class Members paid to Defendants was intended to be used by Defendants to fund adequate security of Defendants' computer property and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for.

114. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their financial and medical accounts and records for misuse.

115. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the cyber-attack. 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 cyber-attack relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

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

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be canceled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

116. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendants, 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 personal and financial information is not accessible online and that access to such data is password-protected.

117. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

118. Plaintiff and Class Members were also injured and damaged by the delayed notice of this data breach, as it exacerbated the substantial and present risk of harm by leaving Plaintiff and Class Members without the knowledge that would have enabled them to take proactive steps to protect themselves.

119. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at present and definitely at increased risk of future harm.

V. CLASS ALLEGATIONS

120. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> National Class: All individuals whose Private Information was compromised as a result of the cyber-attack that Saratoga Harness Racing, Inc. discovered on or about November 1, 2024, and who were mailed the Notice of Data Breach.

121. Excluded from the Class are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

122. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

123. **Numerosity**: The Class is so numerous that the joinder of all members is impracticable. Defendants have identified hundreds of thousands of customers whose Private Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendants' records.

124. **Commonality**: Questions of law and fact common to the Class exist and predominately over any questions affecting only individual Class Members. These include:

a. Whether and when Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Private Information;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' Private Information;

f. Whether Defendants knew or should have known that it did not employ reasonable measures to keep Plaintiff's and Class Members' Private Information secure and prevent loss or misuse of that Private Information;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendants caused Plaintiff and Class Members damages;

i. Whether Defendants violated the law by failing to promptly notify class members that their Private Information had been compromised;

j. Whether Plaintiff and the other Class Members are entitled to credit monitoring and other monetary relief;

125. **Typicality**: Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the data breach, due to Defendants' misfeasance.

126. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

127. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

128. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

129. Likewise, particular issues under Rule 23(c)(4) 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 Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class Members are entitled to actual damages, credit monitoring, or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

130. Plaintiff repeats and re-alleges the allegations set forth in paragraphs 1-129 and incorporates the same as if set forth herein.

131. Defendants required Plaintiff and Class Members to submit non-public personal information in order to obtain services, products, and/or otherwise transact with Defendants.

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

133. Defendants owed a duty of care to Plaintiff 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.

134. Defendants' duty of care to use reasonable security measures arose because Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

135. Defendants owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were the foreseeable and probable victims of any inadequate security practices.

136. Defendants had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

137. Defendants knew, or should have known, that their computer systems and security practices did not adequately safeguard the Private Information of Plaintiff and Class Members.

138. Defendants breached their duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

139. Defendants breached their duties of care by failing to provide prompt notice of the data breach to the persons whose Private Information was compromised.

140. Defendants acted with reckless disregard for the security of the Private Information of Plaintiff and Class Members because Defendants knew or should have known that their computer systems and data security practices were not adequate to safeguard the Private Information that they collected, which hackers targeted in the Data Breach.

141. Defendants acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate notice of the Data Breach so that they could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

142. Defendants had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Defendants with their Private Information was predicated on the mutual understanding that Defendants would implement adequate security precautions. Moreover, Defendants were in an exclusive position to protect their systems (and the Private Information) from attack. Plaintiff and Class Members reasonably relied on Defendants to protect their Private Information.

143. In addition, Defendants 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.

144. Defendants breached their 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 Defendants 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 their networks and systems;

c. Failure to periodically ensure that their network 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;

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

g. Failing to have mitigation and back-up plans in place in the event of a cyber-attack and data breach.

145. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

146. 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.

147. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack and data breach.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and All Class Members)

148. Plaintiff repeats and re-alleges the allegations set forth in paragraphs 1-129 and incorporates the same as if set forth herein.

149. When Plaintiff and Class Members provided their Private Information to Defendants in exchange for Defendants' services and/or products, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

150. Defendants solicited and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their Private Information to Defendants.

151. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

152. Class Members who paid money to Defendants reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Yet Defendants failed to do so.

153. The protection of Plaintiff's and Class Members' Private Information was a material aspect of the implied contracts between Defendants and their customers, including Plaintiff and Class Members.

154. On information and belief, the implied contracts – contracts that include the contractual obligations to maintain the privacy of Plaintiff's and Class Members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendants' applicable privacy policy.

155. Defendants' express representations, including, but not limited to, the express representations found in its applicable privacy policy, memorialize and embody the implied contractual obligation requiring Defendants to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' Private Information.

156. Plaintiff and Class Members would not have entrusted their Private Information to Defendants, nor entered into these implied contracts, without the understanding that their information would be properly safeguarded. They relied on Defendants' implied promise to monitor their computer systems and networks and to implement reasonable data security measures to protect that information.

157. A meeting of the minds occurred, as Plaintiff and Members of the Class agreed to and did provide their Private Information to Defendants and paid for the services and/or products Defendants furnished in exchange for, amongst other things, the protection of their Private Information.

158. Plaintiff and Class Members performed their obligations under the contract when they paid for their services and/or products and provided their valuable Private Information.

159. Defendants materially breached their contractual obligation to protect the nonpublic Private Information Defendants gathered when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

160. Defendants materially breached the terms of the implied contracts. Defendants did not maintain the privacy of Plaintiff's and Class Members' Private Information as evidenced by their notifications of the cyber-attack to Plaintiff and thousands of Class Members. Specifically, Defendants did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA or otherwise protect Plaintiff's and the Class Members' Private Information, as set forth above.

161. The Data Breach was a reasonably foreseeable consequence of Defendants' actions in breach of these contracts.

162. As a result of Defendants' failure to fulfill the data security protections promised in these contracts, Plaintiff and Members of the Class did not receive the full benefit of the bargain and instead received services and/or products that were of a diminished value to that described in the contracts. Plaintiff and Class Members, therefore, were damaged in an amount at least equal to the difference in the value of the services and/or products with data security protection they paid for and the services and/or products they received.

163. Had Defendants disclosed that its security was inadequate or that its did not adhere to industry-standard security measures, neither the Plaintiff, the Class Members, nor any reasonable person would have purchased services and/or products from Defendants.

164. As a direct and proximate result of the cyber-attack/data breach, Plaintiff and Class Members have been harmed and have presently suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendants.

165. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the cyber-attack/data breach.

166. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their 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.

COUNT III
NEGLIGENCE PER SE
(On Behalf of Plaintiff and All Class Members)

167. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 129.

168. Pursuant to Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

169. Plaintiff and Class Members are within the class of persons that the FTCA intended to protect.

170. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued 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 harm as that suffered by Plaintiff and the Class.

171. Defendants breached their duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

172. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

173. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

174. The injury and harm suffered by Plaintiff and Class Members were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they was failing to meet their duties, and that Defendants' breach would cause Plaintiff and

Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

COUNT IV
UNJUST ENRICHMENT
(on behalf of Plaintiff and All Class Members)

176. Plaintiff restates and realleges paragraphs 1 through 129 above as if fully set forth herein and pleads this count in the alternative to the breach of contract count (Count II) above.

177. Upon information and belief, Defendants fund their data security measures entirely from their general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

178. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members 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 Defendants.

179. Plaintiff and Class Members conferred a monetary benefit on Defendants. Rather than using a portion of that benefit to implement reasonable data security measures, Defendants enriched themselves by cutting costs on cybersecurity. Instead of providing adequate protections that could have prevented the cyber-attack, Defendants chose to prioritize profits over the security of Plaintiff's and Class Members' Private Information by employing cheaper, inadequate safeguards. As a direct and proximate result of this decision, Plaintiff and Class Members suffered harm.

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

181. Defendants acquired the Private Information through inequitable means by failing to disclose their inadequate security practices, as previously alleged.

182. If Plaintiff and Class Members knew that Defendants had not secured their Private Information, they would not have agreed to provide their Private Information to Defendants.

183. Plaintiff and Class Members have no adequate remedy at law.

184. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) 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; (vi) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) 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 Plaintiff and Class Members.

185. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

186. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendants' services.

COUNT V
VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law *§§ 349, et seq.*
(on behalf of Plaintiff and All Class Members)

187. Plaintiff and the Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 129.

188. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law ("GBL") § 349, including:

189. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;

a. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, and New York GBL § 349, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;

d. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New York GBL § 349;

e. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and

f. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and New York GBL § 349.

190. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

191. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and Class Members' rights. As mentioned above, data breaches within the hospitality industry put it on notice that its security and privacy protections were inadequate.

192. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendants as they would not have paid Defendants for goods and services or would have paid less for such goods and services but for Defendants' violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; time and money spent cancelling and replacing passports; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

193. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the numerous New Yorkers affected by the Data Breach.

194. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiff and Class Members that they could not reasonably avoid.

195. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, restitution, injunctive relief, and attorney's fees and costs.

COUNT VI
DECLARATORY JUDGMENT
(on behalf of Plaintiff and All Class Members)

196. Plaintiff repeats and re-alleges the allegations set forth in paragraphs 1-129 and incorporates the same as if set forth herein.

197. Defendants owed duties of care to Plaintiff and Class Members, which would require them to adequately secure Private Information.

198. Defendants continue to possess the Private Information of Plaintiff and Class Members, yet have not indicated that they are employing any secure method to safeguard it.

199. Due to Defendants' failure to safeguard the Private Information of Plaintiff and Class Members, such confidential data remains available for sale on the Dark Web or is otherwise publicly accessible, leaving it vulnerable to continued malicious use.

200. Although Defendants claim they have "taken additional steps to further enhance our network security,"[27] there is no detail on what, if any, fixes have really occurred.

201. Plaintiff and Class Members are at risk of harm due to the exposure of their Private Information and Defendants' failure to address the security failings that led to such exposure.

202. There is no reason to believe that Defendants' current security measures are any more adequate than they were prior to the Data Breach, or that they now meet Defendants' contractual obligations and legal duties. Moreover, there is no assurance that other security vulnerabilities do not exist and simply have not yet been discovered or exploited.

203. Plaintiff, seeks a declaration that (1) Defendants' existing security measures fail to comply with their explicit or implicit contractual obligations and duties of care to implement reasonable security procedures and practices appropriate to the nature of the personal information they collect and maintain, and (2) to satisfy these obligations and duties, Defendants must implement and maintain reasonable security measures, including but not limited to:

a. Ordering that Defendants engage 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

[27] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/34543f35-860e-45a8-b59d-8026b2a8c40e.html (last visited May 13, 2025).

a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants' internal network be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants conduct regular database scanning and security checks;

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering Defendants to purchase credit monitoring services for Plaintiff and Class Members for a period of ten years; and

h. Ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their Private Information to third parties, as well as the steps their customers must take to protect themselves.

///

///

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. An Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

B. Equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;

C. Injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

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 personal identifying information of Plaintiff and Class Members 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 Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or

unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. prohibiting Defendants from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vii. 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;

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

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

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

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

xii. 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 personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xiii. 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;

xiv. requiring Defendants to implement a system of tests to assess their 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 personal identifying information;

xv. requiring Defendants to 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;

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs

sufficient to track traffic to and from Defendants' servers; and 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 to report any deficiencies with compliance of the Court's final judgment;

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

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

F. Prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: May 14, 2025

Respectfully Submitted,

By: /s/ *Gregory Haroutunian*
Gregory Haroutunian

Gregory Haroutunian (NDNY Bar Roll No. 704963)
M. Anderson Berry*
Michelle Zhu*
CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Tel: 916.239.4778
Fax: 916.924.1829
aberry@justice4you.com
gharoutunian@justice4you.com
mzhu@justice4you.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice* forthcoming

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

1:25-cv-614

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

MARY DELL PAYNE, individually and on behalf of all others similarly situated

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
M. Anderson Berry; Gregory Haroutunian
Clayeo C. Arnold, APC; 865 Howe Ave., Sacramento, CA 95825; Tel. 916-239-4778; aberry@justice4you.com

DEFENDANTS

SARATOGA HARNESS RACING, INC., and SARATOGA CASINO HOLDINGS LLC

County of Residence of First Listed Defendant Saratoga County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

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

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

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

(For Diversity Cases Only)

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

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

Click here for: Nature of Suit Code Descriptions.

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

TORTS

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

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

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

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

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

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

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

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

PRISONER PETITIONS

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

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

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

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

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

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

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. section 1391 and 28 U.S.C. section 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
May 14, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Gregory Haroutunian

FOR OFFICE USE ONLY

RECEIPT # ANYNDC-7134362 AMOUNT $405 APPLYING IFP _____ JUDGE AMN MAG. JUDGE DJS

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading 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. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.