LYNCH CARPENTER, LLP
Anasuya E. Shekhar (State Bar No. 037403)
Gerald D. Wells, III (*pro hac vice* forthcoming)
1133 Penn Ave, 5th Floor
Pittsburgh, PA 15222
T: 412-322-9243
anasuya@lcllp.com
jerry@lcllp.com

Attorneys for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Dylan Cain, individually and on behalf of all others similarly situated, Plaintiff, v. Barrett-Jackson Holdings, LLC, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff Dylan Cain ("Plaintiff") brings this Class Action Complaint on behalf of himself, and all others similarly situated, against Defendant Barrrett-Jackson Holdings, LLC ("Barrett-Jackson" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

Nature of the Case

1. Plaintiff brings this class action lawsuit on behalf of all persons who entrusted Barrett-Jackson with sensitive Personally Identifiable Information ("PII")[1] and

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79.

Protected Health Information ("PHI") (collectively "Private Information") that was impacted in a data breach that Defendant disclosed to Plaintiff via letter dated on or about July 31, 2025 regarding a breach that occurred on November 25, 2024 (the "Data Breach" or the "Breach").

2. PII and PHI are collectively referred to as "Private Information."

3. Plaintiff's claims arise from Defendant's failure to properly secure and safeguard Private Information that was entrusted to it, and its accompanying responsibility to store and transfer that information.

4. Barrett-Jackson is an American collector car auction company headquartered in Scottsdale, Arizona. It claims to produce "The World's Greatest Collector Car Auctions in Scottsdale, Arizona, and Palm Beach, Florida, where thousands of the most sought-after, unique and valuable automobiles cross the block in front of a global audience.[2]

5. As part of its business, Defendant receives and maintains the PII/PHI of thousands of its current and former customers and employees.

6. Defendant had numerous statutory, regulatory, contractual, and common law duties and obligations, including those based on their affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

7. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "This Privacy Policy explains how information about you is collected, used and disclosed by Barrett-Jackson."

b. "We will also take steps to ensure that the information we collect is treated securely and in accordance with this Privacy Policy, and we have put in place technical and organizational procedures designed

[2] *Company History*, BARRETT-JACKSON, https://www.barrett-jackson.com/company (last visited Aug. 20, 2025).

to safeguard the information we collect."[3]

8. By letter dated July 31, 2025, Defendant revealed to states' Attorneys General that an unauthorized third party gained access to its network.[4]

9. On or about the same time Defendant began notifying affected individuals of the Data Breach.[5]

10. Despite Barrett-Jackson's duty to safeguard the Private Information of its current and previous customers and employees, Plaintiff's and Class Members' Private Information was compromised in a data breach when Defendant determined "that certain files were copied from the system as part of a cyber incident on or around November 25, 2024."[6]

11. Defendant began investigating its systems after it became aware of suspicious activity surrounding its computer systems.[7] After determining a breach had occurred, Defendant undertook an investigation to determine what information had been compromised. This effort lasted until around July 1, 2025.[8]

12. The data breach occurred in part because of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which it was entrusted.

13. Despite having completed its investigation by July 1, 2025, Barrett-Jackson waited almost one month before notifying states' Attorneys General and notifying individuals of the unauthorized access.

14. Based on publicly available information, the Private Information impacted

---

[3] *Privacy Policy*, BARRETT-JACKSON, https://www.barrett-jackson.com/privacyPolicy (last visited Aug. 20, 2025).

[4] *See, e.g.,* https://mm.nh.gov/files/uploads/doj/remote-docs/barrett-jackson-holdings-20250731.pdf (last visited Aug. 20, 2025).

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] *Id.*

by the Data Breach includes a wide swath of highly sensitive information belonging to Barrett-Jackson's current and former customers, including their Social Security numbers; driver's license numbers; passport numbers; bank account numbers; routing numbers; financial documents with account numbers; COVID-19 vaccines and results; health insurance information; and digital signature/authentication names.[9]

15. As a direct and proximate result of Defendant's failure to implement and follow basic security procedures, Plaintiff's and Class Members' Private Information is now exposed to cybercriminals.

16. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, and/or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and timely notice of the Data Breach.

17. Plaintiff and Class Members are now at a significantly increased and certainly impending risk of fraud, identity theft, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiff and Class Members must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

18. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time

[9] *Id.*

incurred due to actual identity theft; (e) deprivation of value of their Private Information; and (f) the continued risk to their sensitive Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect it collected and maintained.

19. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for negligence and negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment arising from the Data Breach. Plaintiff seeks damages and injunctive relief, including the adoption reasonably sufficient practices to safeguard the Private Information in Defendant's custody to prevent incidents like the Data Breach from reoccurring in the future, and for Defendant to provide identity theft protective services to Plaintiff and Class Members for their lifetimes.

20. More specifically, Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

Parties

21. Plaintiff Dylan Cain is an adult, who at all relevant times, was a resident and citizen of the State of Washington. Plaintiff is a former customer of Defendant, who received a data breach notice informing him that his Private Information provided to Barrett-Jackson was compromised during the Data Breach.

22. Plaintiff has suffered actual injury from having his Private Information exposed and/or stolen as a result of the Data Breach, including: (a) required mitigation efforts, including researching the Data Breach and needing to monitor his financial statements to ensure his information is not used for identity theft and fraud; (b) damages to and diminution of the value of his Private Information, a form of intangible property that loses value when it falls into the hands of criminals; (c) loss of privacy; and

(d) continuous imminent and impending injury raising from increased risk of financial identity theft and fraud.

23. As a result of the Data Breach, Plaintiff will continue to be at a substantial and certainly impending risk for fraud and identity theft, and their attendant damages, for years to come.

24. Defendant Barrett-Jackson is a limited liability company formed under the laws of Delaware and with its principal place of business at 15555 North 79th Place, Scottsdale, Arizona 85260.

Jurisdiction and Venue

25. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interest and costs, there are 100 or more members of the proposed class, and at least one member of the proposed class is a citizen of a state different than Defendant.

26. This Court has personal jurisdiction over Defendant because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

27. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District and Defendant resides in this District.

Factual Background

28. Defendant is an auctioneer of motor vehicles and "produces The World's Greatest Collector Car Auctions in Scottsdale, Arizona, and Palm Beach, Florida, where thousands of the most sought-after, unique and valuable automobiles cross the block in front of a global audience."[10]

[10] *Company History*, n. 1.

29. Plaintiff and Class Members are and/or were customers or employees of Defendant.

30. As a condition of participating in one of Defendant's auctions or being in Defendant's employ, Plaintiff and Class Members directly or indirectly entrusted Barrett-Jackson with their sensitive Private Information.

31. Plaintiff and Class Members value the confidentiality of their Private Information and, accordingly, have taken reasonable steps to maintain the confidentiality of their Private Information.

32. In turning over their Private Information, Plaintiff and Class Members reasonably expected that Barrett-Jackson would safeguard their highly sensitive information.

33. By obtaining, collecting, and storing Plaintiff's and Class Members' Private Information, Barrett-Jackson assumed equitable and legal duties to safeguard Plaintiff's and Class Members' highly sensitive information, to only use this information for business purposes, and to only make authorized disclosures.

34. Despite these duties, Barrett-Jackson failed to implement reasonable data security measures to protect Plaintiff's and Class Members' Private Information and ultimately allowed threat actors to breach its computer systems and exfiltrate Plaintiff's and Class Members' Private Information.

35. As a result of the Data Breach, Plaintiff has experienced increased amounts of spam email, texts and phones calls. Further, due to the Data Breach, Plaintiff has spent significant time attempting to monitor and protect his Private Information.

THE VALUE OF PRIVATE INFORMATION AND EFFECTS OF UNAUTHORIZED DISCLOSURE

36. Barrett-Jackson understood that the Private Information it collects was highly sensitive and of significant value to those who would use it for wrongful purposes.

37. Barrett-Jackson also knew that a breach of its computer systems, and

exposure of the Private Information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

38. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred at business such as Equifax, Facebook, Yahoo, Marriott, Anthem, and many others.

39. Private Information has considerable value and constitutes an enticing and well-known target to hackers. Hackers easily can sell stolen data as there has been "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[11]

40. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[12]

41. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. In 2021, there were 4,145 publicly disclosed data breaches, exposing 22 billion records. The United States specifically saw a 10% increase in the total number of data breaches.[13]

42. Indeed, a 2022 poll of security executives predicted an increase in attacks over the next two years from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will

---

[11] Brian Krebs, *The Value of a Hacked Company*, Krebs on Security (July 14, 2016), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/ (last visited August 20, 2025).

[12] *What To Know About Identity Theft*, FTC Consumer Advice (Sept. 2024), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited August 20, 2025).

[13] *Data Breach Report: 2021 Year End*, Risk Based Security (Feb. 4, 2022), https://www.scribd.com/document/574129638/2021-Year-End-Data-Breach-QuickView-Report (last visited August 20, 2025).

largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[14]

43. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, 2024 had the second-highest number of data compromises in the U.S. in a single year since such instances began being tracked in 2005.[15]

44. The ramifications of Barrett-Jackson's failure to keep Plaintiff's and Class Members' Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] 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."[16]

45. Even if stolen Private Information does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known

---

[14] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need to Know*, Forbes (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed August 20, 2025).

[15] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20, (last visited August 20, 2025).

[16] U.S. Gov't Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited August 20, 2025).

as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

46. The specific types of personal data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Plaintiff and other Class Members especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

47. **Social Security Numbers**—Unlike credit or debit card numbers in a payment card data breach—which can quickly be frozen and reissued in the aftermath of a breach—unique Social Security Numbers cannot be easily replaced. Even when such numbers are replaced, the process of doing so results in a major inconvenience to the subject person, requiring a wholesale review of the person's relationships with government agencies and any number of private companies in order to update the person's accounts with those entities.

48. Indeed, the Social Security Administration warns that the process of replacing a Social Security is a difficult one that creates other types of problems, and that it will not be a complete remedy for the affected person:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.

> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[17]

49. Social Security Numbers allow individuals to apply for credit cards, student loans, mortgages, and other lines of credit—among other services. Often social security numbers can be used to obtain medical goods or services, including prescriptions. They are also used to apply for a host of government benefits. Access to such a wide range of assets makes social security numbers a prime target for cybercriminals and a particularly attractive form of PII to steal and then sell.

50. **Passport Numbers**—As explained by Aura, a leading identity theft protection service, "[p]assports are among the most widely accepted forms of identification, making them prime targets for scammers and fraudsters. If scammers steal your passport number, they can impersonate you, create fake travel documents, or even open bank accounts in your name."[18] Indeed, when combined with other PII, such as a name, address, or picture, a "passport number enables scammers to impersonate you, access your online accounts, or target you in sophisticated scams that lead to identity theft."[19]

51. Moreover, "[u]nlike credit card data or personal Social Security numbers, there are few mechanisms in place to alert consumers that their passport numbers have

---

[17] *Identify Theft and Your Social Security Numbers*, Social Security Admin. (June 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited August 20, 2025).

[18] Yaniv Masjedi, *What Can Scammers Do With Your Passport Number*?, Aura (Apr. 12, 2023), https://www.aura.com/learn/what-can-someone-do-with-your-passport-number#:~:text=If%20scammers%20steal%20your%20passport,could%20still%20be%20at%20risk (last visited August 20, 2025).

[19] *Id.*

been stolen and possibly used for fraud" making it difficult to determine if criminals are using a forged or fraudulent passport in an individual's name.[20]

52. Based on the value to cybercriminals of the PII in its possession, Barrett-Jackson knew or should have known the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. Barrett-Jackson failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

BARRETT-JACKSON BREACHED ITS DUTY TO PROTECT PRIVATE INFORMATION

53. Barrett-Jackson became aware of suspicious activity related to some of its computer systems. After which it initiated an investigation and determined that certain files were copied from the system as part of a cyber incident on or around November 25, 2024.[21]

54. The Private Information impacted by the Data Breach includes a wide swath of highly sensitive information belonging to Barrett-Jackson's current and former customers and employees, including their names, birth dates, addresses, Social Security numbers (SSNs), Tax ID numbers, and images of checks. The exposed data also included medical conditions, treatments and test results, dates of birth, and Social Security numbers.[22]

55. On or around July 31, 2025, nearly one month after the Data Breach was discovered, Barrett-Jackson reported the Data Breach to the offices of various states' Attorneys General and indicated it was also notifying affected individuals.[23]

---

[20] Kate Fazzini, *Here's how criminals use stolen passport information*, CNBC (July 5, 2019), https://www.cnbc.com/2019/07/05/how-criminals-use-stolen-passport-information.html (last visited August 20, 2025).

[21] https://mm.nh.gov/files/uploads/doj/remote-docs/barrett-jackson-holdings-20250731.pdf (last accessed August 20, 2025).

[22] *Id.*

[23] *Id.*

56. Importantly, this notice took place 248 days after the Data Breach began.

57. As a result, Defendant kept Plaintiff and Class Members in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

58. As set forth herein, despite this threat, and other known threats, upon information and belief, Barrett-Jackson failed to take any action to increase security of the Private Information it held and knew to be highly valuable to cybercriminals.

59. Shortly after Barrett-Jackson started notifying Attorneys General of the Data Breach, Plaintiff received a notice informing him that his Private Information had been compromised during the Data Breach.

60. Upon information and belief, Class Members received similar notices informing them that their Private Information was compromised during the Data Breach.

61. While Defendant has yet to fully determine the breadth of the Data Breach, it has issued over 3,500 notices to individuals in six states.[24]

62. The Data Breach occurred as a direct result of Barrett-Jackson's failure to implement and follow basic security procedures to protect its current and former customers' and employees' Private Information that it had collected and stored.

BARRETT-JACKSON FAILED TO COMPLY WITH FTC GUIDELINES

63. Barrett-Jackson is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[24] *Barrett-Jackson Data Breach Exposes Social Security Numbers*, ClaimDepot, https://www.claimdepot.com/data-breach/barrett-jackson-2025 (last accessed August 20, 2025).

64. The 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.[25]

65. Among other guidance, the FTC recommends the following cybersecurity guidelines for businesses in order to protect sensitive information in their systems: [26]

a. Identify all connections to the computers where sensitive information is stored;

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates

[25] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed August 20, 2025).

[26] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed August 20, 2025).

the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business's network, the transmission should be investigated to make sure it is authorized.

66. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[27]

67. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

68. Barrett-Jackson failed to properly implement basic data security practices. Barrett-Jackson's failure to employ reasonable and appropriate measures to protect against

[27] *Id.*

unauthorized access to its customers' and employees' Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

69. Barrett-Jackson was at all times fully aware of its obligations to protect the Private Information of its customers and employees given the reams of Private Information that it had access to. Barrett-Jackson was also aware of the significant repercussions that would result from a failure to properly secure the Private Information it maintained.

BARRETT-JACKSON FAILURE TO PREVENT, IDENTIFY, AND TIMELY REPORT THE DATA BREACH

70. Barrett-Jackson admits that an unauthorized third party accessed it information technology system.

71. Barrett-Jackson failed to take necessary precautions or employ adequate measures necessary to protect its computer systems against unauthorized access and keep Plaintiff's and Class Members' Private Information secure.

72. The Private Information that Barrett-Jackson allowed to be exposed in the Data Breach is the type of private information that Barrett-Jackson knew or should have known would be the target of cyberattacks.

73. Despite its own knowledge of the inherent risks of cyberattacks, and notwithstanding the FTC's data security principles and practices,[28] Barrett-Jackson failed to disclose that its systems and security practices were inadequate to reasonably safeguard individuals' Private Information.

74. The FTC directs businesses to use an intrusion detection system to expose a breach as soon as it occurs, monitor activity for attempted hacks, and have an immediate

[28] Protecting Personal Information: A Guide for Business, Fed. Trade Comm'n (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited August 20, 2025).

response plan if a breach occurs.[29] Immediate notification to individuals impacted by a data breach is critical so that those impacted can take measures to protect themselves.

75. Here, Barrett-Jackson inexcusably waited for months after the Data Breach occurred to notify impacted individuals.

THE DATA BREACH'S INCLUSION OF PHI IS PARTICULARLY SIGNIFICANT

76. With respect to the data breaches implicating PHI, a study found "the majority [70%] of data impacted by healthcare breaches could be leveraged by hackers to commit fraud or identity theft."[30]

77. "Actors buying and selling PII and PHI from healthcare institutions and providers in underground marketplaces is very common and will almost certainly remain so due to this data's utility in a wide variety of malicious activity ranging from identity theft and financial fraud to crafting of bespoke phishing lures."[31]

78. The reality is that cybercriminals seek nefarious outcomes from a data breach and "stolen health data can be used to carry out a variety of crimes."[32]

79. Health information in particular is likely to be used in detrimental ways—by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.[33]

80. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in

---

[29] *Id.*

[30] *70% Of Data Involved In Healthcare Breaches Increases Risk Of Fraud*, DistilINFO (Oct. 3, 2019), https://distilgovhealth.com/2019/10/03/70-of-data-involved-in-healthcare-breaches-increases-risk-of-fraud/ (last visited August 20, 2025).

[31] *Id.*

[32] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HealthTech (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited August 20, 2025).

[33] *Id.*

one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[34]

81. The "high value of medical records on the dark web has surpassed that of social security and credit card numbers. These records can sell for up to $1,000 online . . ."[35]

82. Cybercriminals sell health information at a far higher premium than stand-alone PII. This is because health information enables thieves to go beyond traditional identity theft and obtain medical treatments, purchase prescription drugs, submit false bills to insurance companies, or even undergo surgery under a false identity. The shelf life for this information is also much longer—while individuals can update their credit card numbers, they are less likely to change their health insurance information. When medical identity theft occurs, the associated costs to victims can be exorbitant. According to a 2015 study, at least 65% of medical identity theft victims had to "pay an average of $13,500 to resolve the crime."[36]

83. As noted above, some of the information that was compromised in the Data Breach included, among other things, health insurance information and COVID-19 testing results and vaccine status. Accordingly, Plaintiff and Class Members must remain especially vigilant given the highly sensitive nature of the PHI at issue in this Data Breach.

BARRETT-JACKSON FAILED TO COMPLY WITH HIPAA'S MANDATES

84. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160

---

[34] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDExperts (May 14, 2015), https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited August 20, 2025).

[35] Steger, n. 32.

[36] Justin Klawans, *What is treatment identity theft and how can you avoid it?*, The Week (Aug. 2, 2023), https://theweek.com/feature/briefing/1025328/medical-identity-theft-how-to-avoid (last visited August 20, 2025).

and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

85. In addition, Barrett-Jackson is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

86. HIPAA's Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information, while HIPAA's Security Standards for the Protection of Electronic Protected Health Information establishes national security standards for health information that is stored or transmitted electronically.

87. HIPAA requires "comply[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302. Such health information includes "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

88. HIPAA's Security Rule requires entities such as Barrett-Jackson to, *inter alia*, do the following: (i) ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; (ii) protect against any reasonably anticipated threats or hazards to the security or integrity of such information; (iii) protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and (iv) ensure compliance by its workforce.

89. HIPAA also requires entities such as Barrett-Jackson to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Barrett-Jackson is required under HIPAA to "[i]implement technical

policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

90. Moreover, both HIPAA and HITECH required Barrett-Jackson to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

91. Finally, HIPAA requires an entity to provide notice of a data breach to affected individuals "without unreasonable delay and in no case later than 60 days following discovery of the breach." 45 C.F.R. §§ 164.400-414.

92. Barrett-Jackson was, at all times, aware of the mandates of HIPAA. Despite being aware of these mandates and its concomitant obligations, Barrett-Jackson failed to comply with its obligations and protect the PHI of Plaintiff and the Class Members. Defendant's failure in this regard is especially egregious given that Defendant was fully aware of the breadth and depth of PHI it obtained and stored and the foreseeable consequences that would result from unauthorized disclosure of this information.

PLAINTIFF AND CLASS MEMBERS SUFFERED DAMAGES

93. The ramifications of Barrett-Jackson's failure to keep Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

94. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

95. Plaintiff and Class Members are at substantial increased risk of suffering identity theft and fraud or misuse of their Private Information as a result of the Data Breach. From a recent study, 28% of individuals affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[37]

96. Further, Plaintiff and Class Members have incurred and will incur out of pocket costs for protective measures, such as identity theft protection, credit monitoring, credit report fees, credit freeze fees, and similar costs related to the Data Breach.

97. Besides the monetary damage sustained in the event of identity theft, consumers may have to spend hours trying to resolve identity theft issues. For example, the FTC estimates that it takes consumers an average of 200 hours of work over approximately six months to recover from identity theft.[38]

98. Plaintiff and Class Members are also at a continued risk because their information remains in Barrett-Jackson's systems, which the Data Breach showed are susceptible to compromise and attack and are subject to further attack so long as Barrett-Jackson fails to take necessary and appropriate security and training measures to protect the Private Information in its possession.

99. Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their Private Information to strangers.

---

[37] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KnowBe4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last accessed August 18, 2025).

[38] Cepeda Cheeks, *How to Report identity Theft*, ConsumerAffairs (Feb. 17, 2022), https://www.consumeraffairs.com/finance/how-to-report-identity-theft.html (last accessed August 20, 2025).

100. As a result of Barrett-Jackson's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including out of pocket expenses; loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable Private Information; the imminent and certainly impeding injury flowing from fraud and identity theft posed by their Private Information being disclosed to unauthorized recipients and cybercriminals; damages to and diminution in value of their Private Information; and continued risk to Plaintiff's and the Class Members' Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Barrett-Jackson fails to undertake appropriate and adequate measures to protect the Private Information entrusted to it.

Class Allegations

101. Plaintiff brings this class action on behalf of himself and all other individuals who are similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure.

102. Plaintiff seeks to represent a class of persons to be defined as follows:

> All individuals in the United States whose Private Information was compromised in the Data Breach (the "Class").

103. Excluded from the Class are Barrett-Jackson, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

104. This proposed class definition is based on the information available to Plaintiff at this time. Plaintiff may modify the class definition in an amended pleading or when he moves for class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

105. **Numerosity:** Plaintiff is informed and believes, and thereon alleges, that there are at minimum, thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendant's records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes thousands of individuals.

106. **Commonality:** This action involved questions of law and fact common to the Class. Such common questions include but are not limited to:

a. Whether Defendant had a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' Private Information, and breached its duties thereby;

c. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct; and

d. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

107. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class were all customers or employees of Defendant, and each had their Private Information exposed and/or accessed by an unauthorized third party.

108. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the

prosecution of class action litigation. The claims of Plaintiff and the Class Members are substantially identical as explained above.

109. **Superiority:** This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Class is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense, and promote uniform decision-making.

110. **Predominance:** Common questions of law and fact predominate over any questions affecting only individual Class Members. Similar or identical violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action. For example, Defendant's liability and the fact of damages are common to Plaintiff and each member of the Class. If Defendant breached its duty to Plaintiff and Class Members, then Plaintiff and each Class member suffered damages by that conduct.

111. **Injunctive Relief:** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. R. Civ. P. 23(b)(2).

112. **Ascertainability:** Members of the Class are ascertainable. Class membership is defined using objective criteria, and Class Members may be readily identified through Defendant's books and records.

CLAIMS FOR RELIEF

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

113. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

114. Plaintiff and Class Members provided their non-public Private Information to Defendant as a condition of obtaining employment from Defendant or participating in an auction.

115. Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in securing, safeguarding, storing, and protecting the PII and PHI it collected from being compromised, lost, stolen, accessed and misused by unauthorized parties. This duty includes, among other things, designing, maintaining, overseeing, and testing Defendant's security systems to ensure that PII and PHI in Barrett-Jackson's possession was adequately secured and protected

116. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

117. Defendant owed a duty of care to Plaintiff and Class Members to provide reasonable security, consistent with industry standards, to ensure that its systems and networks adequately protected their Private Information.

118. Defendant had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust Barrett-Jackson with their Private Information as a condition of working for Defendant are participating in one of its auctions was predicated on the understanding that Barrett-Jackson would take adequate security precautions to protect their PII and PHI.

119. By assuming the responsibility to collect and store this data, Defendant had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

120. Plaintiff and members of the Class entrusted Defendant with their PII and PHI with the understanding that Barrett-Jackson would safeguard their information.

121. Defendant's conduct also created a foreseeable risk of harm to Plaintiff and Class Members by failing to: (1) secure its systems and exercise adequate oversight of its data security protocols; (2) ensure compliance with industry standard data security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

122. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and PHI, the vulnerabilities of its systems, and the importance of adequate security. Defendant should have been aware of numerous, well-publicized data breaches in the months and years preceding the Data Breach.

123. Defendant breached its common law duty to act with reasonable care in collecting and storing the Private Information of its customers and employees, which exists independently from any contractual obligations between the parties. Specifically, Defendant breached its common law, statutory, and other duties to Plaintiff and Class Members in numerous ways, including by:

a. failing to adopt reasonable data security measures, practices, and protocols;

b. failing to implement data security systems, practices, and protocols sufficient to protect Plaintiff's and Class Members' PII and PHI;

c. storing PII and PHI longer than reasonably necessary;

d. failing to comply with industry-standard data security measures; and

e. failing to timely disclose critical information regarding the nature of the Data Breach.

124. Defendant's failure to implement and maintain adequate data security measures to protect Plaintiff's and Class Members' Private Information created conditions conducive to a foreseeable, intentional criminal act in the form of the Data Breach. Plaintiff and Class Members did not contribute to the Data Breach or the subsequent misuse of their Private Information.

125. Defendant 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 their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

126. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and Class Members of the Data Breach.

127. Defendant had and continues to have duties to adequately disclose that the Private Information of Plaintiff and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice is necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

128. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

129. Defendant has acknowledged that the Private Information of Plaintiff and Class Members was disclosed to unauthorized third persons as a result of the Data Breach.

130. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

131. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

132. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have and will suffer damages including, but not limited to: (i) the loss of value of their Private Information and loss of opportunity to determine for themselves how their PII and PHI are used; (ii) the publication and/or theft of their PII and PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iv) lost opportunity costs associated with 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 tax fraud and identity theft; (v) time, effort, and expense associated with placing fraud alerts or freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII and PHI, which remains in Defendant's possession and are subject to further unauthorized disclosures so long as Barrett-Jackson fails to undertake appropriate and adequate measures to protect it; and (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised for the rest of their lives.

133. But for Defendant's wrongful and negligent breaches of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

134. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding

such Private Information by adopting, implementing, and maintaining appropriate security measures.

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

136. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

137. In addition, Barrett-Jackson had a duty to employ reasonable security measures under Section 5 of the FTC 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.

138. Further, Barrett-Jackson had a duty under HIPAA to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the health care and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

139. Defendant's violation of federal statutes, including the FTC Act and HIPAA, constitutes negligence *per se*.

140. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

141. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

142. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

143. In connection with obtaining employment from Defendant or participating in an auction, Plaintiff and Class Members entered into implied contracts with Barrett-Jackson.

144. Plaintiff and Class Members were required to deliver their Private Information to Defendant as part of their relationship with Defendant.

145. Defendant solicited, offered, and invited Class Members to provide their Private Information. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

146. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing employment or participation in an auction to Plaintiff and Class Members.

147. When Plaintiff and Class Members provided their PII and PHI to Barrett-Jackson, either directly or indirectly, as a pre-condition, they entered into implied contracts with Barrett-Jackson.

148. Pursuant to these implied contracts, in exchange for the consideration and PII and PHI provided by Plaintiff and Class Members, Defendant agreed to, among other things, and Plaintiff and Class Members understood that Barrett-Jackson would: (1) provide products and/or services to Plaintiff and Class Members; (2) implement reasonable measures to protect the security and confidentiality of Plaintiff's and Class Members' PII and PHI; and (3) protect Plaintiff's and Class Members' PII and PHI in compliance with federal and state laws and regulations and industry standards

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

150. Implicit in the agreement between Plaintiff and Class Members and Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

151. The protection of PII and PHI was a material term of the implied contracts between Plaintiffs and Class Members, on the one hand, and Defendant, on the other hand. Indeed, as set forth herein, Defendant recognized its duty to provide adequate data security and ensure the privacy of with its practice of providing a privacy policy on its website.

152. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendant with their PII and PHI.

153. Defendant breached its obligations under its implied contracts with Plaintiff and Class Members in failing to implement and maintain reasonable security measures to protect and secure their PII and PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class Members' PII and PHI in a manner that complies with applicable laws, regulations, and industry standards

154. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

155. On information and belief, at all relevant times, Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

156. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

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

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

159. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

160. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their Private Information, by failing to delete the

information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that Private Information was compromised as a result of the Data Breach

161. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of Private Information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

162. Defendant's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach and the injuries that Plaintiff and Class Members have suffered from the Data Breach.

163. Plaintiff and Class Members suffered by virtue of Defendant's breach of their implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII and PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII and PHI has been breached; (v) they were deprived of the value of their PII and PHI, for which there is a well-established national and international market; (vi) they have lost time and incurred expenses, and will incur future costs to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) they have overpaid for the services they received without adequate data security.

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

165. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures;

(ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

166. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

167. This count is plead in the alternative to the breach of implied contract count above.

168. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

169. Plaintiff and Class Members conferred a benefit on Defendant, whereby they provided their Private Information to Defendant.

170. Defendant prior to and at the time Plaintiff and Class Members entrusted it with their PII and PHI, caused Plaintiff and Class Members to reasonably believe that it would keep that Private Information secure.

171. The monies Defendant was paid in its ordinary course of business included a premium for Defendant's cybersecurity obligations and were supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiff's and Class Members' Private Information.

172. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

173. Defendant failed to disclose facts pertaining to its substandard information systems, or defects and vulnerabilities therein before Plaintiff and Class Members made their decisions to provide Defendant with their Private Information.

174. Defendant enriched itself by hoarding the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profit at the expense of Plaintiff and Class Members by utilizing cheap, ineffective security measures and diverting those funds to its own personal use. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

175. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiff and Class Members, and as a result, Defendant was overpaid.

176. Under principles of equity and good conscience, Defendant should not be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

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

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

179. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be

accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

COUNT IV
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

180. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

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

182. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and Class Members' Private Information and whether Barrett-Jackson is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Private Information. Plaintiff alleges that Barrett-Jackson's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his Private Information will occur in the future.

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

a. Barrett-Jackson owes a legal duty to secure Private Information and to timely notify impacted individuals of a data breach under the common law, HIPAA, and various state statutes; and

b. Barrett-Jackson continues to breach this legal duty by failing to employ reasonable measures to secure Private Information in its possession.

184. This Court also should issue corresponding prospective injunctive relief requiring Barrett-Jackson to employ adequate security protocols consistent with law and industry standards to protect Private Information in Barrett-Jackson's data network.

185. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Barrett-Jackson. The risk of another such breach is real, immediate, and substantial. If another breach at Barrett-Jackson occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and he will be forced to bring multiple lawsuits to rectify the same conduct.

186. The hardship to Plaintiff if an injunction is not issued exceeds the hardship to Barrett-Jackson if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Barrett-Jackson of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Barrett-Jackson has a pre-existing legal obligation to employ such measures.

187. Issuance of the requested injunction will not disserve the public interest. In contrast, such an injunction would benefit the public by preventing another data breach at Barrett-Jackson, thus eliminating the additional injuries that would result to Plaintiff and Class Members whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action, appointing Plaintiff as class representatives for the Class, and appointing Plaintiff's counsel to represent the Class;

B. For equitable relief enjoining Barrett-Jackson from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII and PHI, and from refusing to issue prompt, complete

and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Barrett-Jackson to utilize appropriate methods and policies with respect to data collection, storage, and safety, and to disclose with specificity the types of PII and PHI compromised as a result of the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Barrett-Jackson's wrongful conduct;

E. Ordering Barrett-Jackson to pay for not less than ten years of credit monitoring services for Plaintiff and Class Members;

F. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

G. For an award of punitive damages, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: August 20, 2025

Respectfully submitted,

/s/ Anasuya E. Shekhar
Anasuya E. Shekhar (State Bar No. 037403)
Gerald D. Wells, III*
LYNCH CARPENTER, LLP
1133 Penn Ave, 5th Floor
Pittsburgh, PA 15222
T: 412-322-9243
anasuya@lcllp.com
jerry@lcllp.com

Attorney for Plaintiff and the Proposed Class
**Pro hac vice* forthcoming

UNITED STATES DISTRICT COURT DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): **Dylan Cain , ;**

County of Residence: Outside the State of Arizona

County Where Claim For Relief Arose: Outside the State of Arizona

Plaintiff's Atty(s):

Anasuya E. Shekhar ,
Lynch Carpenter, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
(412) 322-9243

Defendant(s): **Barrett-Jackson Holdings, LLC , ;**

County of Residence: Maricopa

Defendant's Atty(s):

,

,

IFP REQUESTED

REMOVAL FROM COUNTY, CASE #

II. Basis of Jurisdiction: **4. Diversity (complete item III)**

III. Citizenship of Principal Parties**(Diversity Cases Only)**

Plaintiff:- **2 Citizen of Another State**

Defendant:- **4 AZ corp or Principal place of Bus. in AZ**

IV. Origin : **1. Original Proceeding**

V. Nature of Suit: **190 Other Contract**

VI.Cause of Action: **28 U.S.C. § 1332(d)(2)(A). Data Breach.**

VII. Requested in Complaint

Class Action: **Yes**

Dollar Demand: **5000001**

Jury Demand: **Yes**

VIII. This case **IS RELATED** to Case Number **2:25-cv-02893** assigned to Judge **Dominic W. Lanza.**

Signature: /s/ Anasuya E. Shekhar

Date: 8/20/2025

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014