Cristina Perez Hesano (#027023)
PEREZ LAW GROUP, PLLC
7508 North 59th Avenue
Glendale, Arizona 85301
Telephone: (602) 730-100
Fax: (602) 612-6266
cperez@perezlawgroup.com

additional counsel listed below

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

Steven Swinnerton, on behalf of himself and all others similarly situated, Plaintiff, v. **Barrett-Jackson Holdings, LLC**, Defendant.	No. **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

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

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. 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."[1]

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI")—together "PII/PHI"—about its current and former customers. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown for precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former customers' and employees' PII/PHI.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and

[1] *Company*, BARRETT-JACKSON, https://www.barrett-jackson.com/company (last visited Aug. 8, 2025).

failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Defendant's failures placed the Class's PII/PHI in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiff is a Data Breach victim, having received a breach notice—attached as Exhibit A. He brings this class action on behalf of himself, and all others harmed by Defendant's misconduct.

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

PARTIES

8. Plaintiff, Steven Swinnerton, is a natural person and citizen of Phoenix, Arizona where he intends to remain.

9. Defendant, Barrett-Jackson Holdings, LLC, 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

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5

million, exclusive of interest and costs. Members of the proposed Class are citizens of different states than Defendant. [2] For example, there are 1,794 Class Members in Texas.[3]

11. This Court has personal jurisdiction over Defendant because it is headquartered in Arizona, regularly conducts business in Arizona, and has sufficient minimum contacts in Arizona.

12. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII/PHI of Plaintiff and the Class

13. 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."[4]

[2] Under the Class Action Fairness Act, "an unincorporated association shall be deemed to be a citizen of the State where it has its principal place of business and the State under whose laws it is organized." 28 U.S.C. § 1332(d)(10); *See also Minor v. Favorite World LLC* , No. CV 24-4425, 2024 U.S. Dist. LEXIS 102803, at *1 (C.D. Cal. June 10, 2024); *Davis v. HSBC Bank Nevada NA*, 557 F.3d 1026, 1032, & n.13 (9th Cir. 2009) (Kleinfeld, J., concurring) (discussing in dicta) Thus, as an LLC, Defendant Barrett-Jackson Holdings, LLC is a citizen of Delaware (state of formation) and Arizona (principal place of business).

[3] *Data Security Breach Reports*, TEXAS ATTY GEN, https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited Aug. 8, 2025)

[4] *Company*, BARRETT-JACKSON, https://www.barrett-jackson.com/company (last visited Aug. 8, 2025).

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

15. In collecting and maintaining the PII/PHI, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII/PHI.

16. Under state and federal law, businesses like Defendant have duties to protect its current and former customers' and employees' PII/PHI and to notify them about breaches.

17. 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."[5]

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 to safeguard the information we collect."[6]

Defendant's Data Breach

18. On or around November 25, 2024, Defendant was hacked in the Data Breach.[7]

[5] *Privacy Policy*, BARRETT-JACKSON, https://www.barrett-jackson.com/privacyPolicy (last visited Aug. 8, 2025).
[6] *Id*.
[7] *Notice of Data Event*, NEW HAMPSHIRE ATTY GEN (July 31, 2025) https://mm.nh.gov/files/uploads/doj/remote-docs/barrett-jackson-holdings-20250731.pdf.

19. Worryingly, Defendant already admitted that "certain files were copied from the system as part of a cyber incident on or around November 25, 2024."[8]

20. Because of Defendant's Data Breach, at least the following types of PII/PHI were compromised:

a. Social Security numbers;

b. driver's license numbers;

c. passport numbers;

d. bank account numbers;

e. routing numbers;

f. financial documents with account numbers;

g. COVID-19 vaccines and results;

h. health insurance information; and

i. digital signature/authentication.[9]

21. Currently, the precise number of persons injured is unclear. But upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. And upon information and belief, the putative class is over one hundred members—as it includes its current and former customers.

22. And yet, Defendant waited until July 31, 2025, before it began notifying the class—a ***full 248 days*** after the Data Breach began.[10]

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

23. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

24. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

a. "We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors."[11]

25. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant caused widespread injury and monetary damages.

26. Since the breach, Defendant claims that "[w]e recognize the evolving nature of cybersecurity and will continue to evaluate and enhance our existing security measures."[12]

27. But such simple declarations are insufficient to ensure that Plaintiff's and Class Members' PII/PHI will be protected from additional exposure in a subsequent data breach.

[11] *Id.*
[12] *Id.*

28. Further, the Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

29. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity related services. But upon information and belief, such services are wholly insufficient to compensate Plaintiff and Class Members for the injuries that Defendant inflicted upon them.

30. Because of Defendant's Data Breach, the sensitive PII/PHI of Plaintiff and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class Members.

Plaintiff's Experiences and Injuries

31. Plaintiff Steven Swinnerton is a former employee of Defendant.

32. Thus, Defendant obtained and maintained Plaintiff's PII/PHI.

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

34. Plaintiff is very careful about the privacy and security of his PII/PHI. He does not knowingly transmit his PII/PHI over the internet in an unsafe manner. He is careful to store any documents containing his PII/PHI in a secure location.

35. As a condition of his employment with Defendant, Plaintiff provided Defendant with his PII/PHI. Defendant used that PII/PHI to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII/PHI in order to obtain employment and payment for that employment.

36. Plaintiff provided his PII/PHI to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

37. Plaintiff reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII/PHI.

38. Plaintiff received a Notice of Data Breach on or around August 8, 2025.

39. Thus, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

40. Through its Data Breach, Defendant compromised Plaintiff's PII/PHI.

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

42. And in the aftermath of the Data Breach, Plaintiff suffered from a spike in spam and scam emails, text messages and phone calls.

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

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

45. Plaintiff suffered actual injury from the exposure and theft of his PII/PHI—which violates his rights to privacy.

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

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

48. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

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

Consumers Prioritize Data Security

50. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[13] Therein, Cisco reported the following:

a. "For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved

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

from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[14]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[15]

c. 89% of consumers stated that "I care about data privacy."[16]

d. 83% of consumers declared that "I am willing to spend time and money to protect data" and that "I expect to pay more" for privacy.[17]

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."[18]

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."[19]

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

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

[14] *Id*. at 3.
[15] *Id*.
[16] *Id*. at 9.
[17] *Id*.
[18] *Id*.
[19] *Id*. at 11.

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

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

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

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

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

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

53. The value of Plaintiff and Class's PII/PHI on the black market is considerable. Stolen PII/PHI trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

54. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII/PHI far and wide.

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

56. The development of "Fullz" packages means that the PII/PHI exposed in the Data Breach can easily be linked to data of Plaintiff and the Class that is available on the internet.

57. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class Members' stolen PII/PHI is being misused, and that such misuse is fairly traceable to the Data Breach.

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

59. Defendant's failure to promptly and properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII/PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

61. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[20]

62. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[21]

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

---

[20] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

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

Defendant Failed to Follow FTC Guidelines

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

65. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[22] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

67. Furthermore, the FTC explains that companies must:

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

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

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

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

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

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

Defendant Failed to Follow Industry Standards

70. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

72. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

73. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

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

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Barrett-

Jackson in November 2024, including all those individuals who received notice of the breach.

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

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

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

78. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

79. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable. Upon information and belief, the proposed Class includes at least 100 members.

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

81. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. His interests do not conflict with Class Members' interests. And

Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

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

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

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

c. if Defendant were negligent in maintaining, protecting, and securing PII/PHI;

d. if Defendant breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

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

f. if Defendant's Breach Notice was reasonable;

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

h. what the proper damages measure is; and

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

83. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

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

84. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

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

87. Defendant has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

88. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiff and Class Members' PII/PHI.

89. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

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

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class Members within a reasonable timeframe of any breach to the security of their PII/PHI.

90. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiff and Class Members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

91. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

92. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII/PHI of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

93. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

94. The risk that unauthorized persons would attempt to gain access to the PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII/PHI, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII/PHI —whether by malware or otherwise.

95. PII/PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class Members' and the importance of exercising reasonable care in handling it.

96. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

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

98. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class Members' PII/PHI by:

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

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

99. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII/PHI of Plaintiff and Class Members which actually and proximately caused the Data Breach and Plaintiff and Class Members' injury.

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

101. Defendant has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

102. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and Class Members have suffered or will suffer damages, including

monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

103. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

104. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiff and the Class)

105. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

106. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII/PHI.

107. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the

PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class Members' sensitive PII/PHI.

108. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII/PHI.

109. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII/PHI Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

110. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

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

112. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would

cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII/PHI.

113. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

114. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

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

115. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

116. Plaintiff and Class Members were required to provide their PII/PHI to Defendant as a condition of receiving services and/or employment provided by Defendant. Plaintiff and Class Members provided their PII/PHI to Defendant or its third-party agents in exchange for Defendant's services and/or employment.

117. Plaintiff and Class Members reasonably understood that a portion of the funds they paid and/or derived from their labor would be used to pay for adequate cybersecurity measures.

118. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

119. Plaintiff and the Class Members accepted Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in exchange for services and/or employment.

120. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII/PHI to unauthorized persons.

121. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

122. Implicit in the parties' agreement was that Defendant would provide Plaintiff and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

123. After all, Plaintiff and Class Members would not have entrusted their PII/PHI to Defendant in the absence of such an agreement with Defendant.

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

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

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

127. Defendant materially breached the contracts it entered with Plaintiff and Class Members by:

a. failing to safeguard their information;

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

c. failing to comply with industry standards;

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

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Defendant created, received, maintained, and transmitted.

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

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

130. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

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

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

133. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII/PHI and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

134. Defendant owed a duty to its current and former customers, including Plaintiff and the Class, to keep this information confidential.

135. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII/PHI is highly offensive to a reasonable person.

136. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

137. The Data Breach constitutes an intentional interference with Plaintiff's and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

138. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

139. Defendant acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

140. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

141. As a proximate result of Defendant's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

142. And, on information and belief, Plaintiff's PII/PHI has already been published—or will be published imminently—by cybercriminals on the Dark Web.

143. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Defendant with their inadequate cybersecurity system and policies.

144. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII/PHI of Plaintiff and the Class.

145. In addition to injunctive relief, Plaintiff, on behalf of himself and the other Class Members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future

monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

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

146. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

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

148. Plaintiff and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from (1) using their PII/PHI to provide services and/or facilitate employment, and (2) accepting payment and/or using their labor to derive profit.

149. Defendant appreciated or had knowledge of the benefits it received from Plaintiff and Class Members.

150. Plaintiff and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

151. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII/PHI.

152. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper,

ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

153. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII/PHI and (2) employment and/or payment because Defendant failed to adequately protect their PII/PHI.

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

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

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

156. Plaintiff incorporates by reference all other paragraphs as if fully set forth herein.

157. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

158. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiff alleges that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class Members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class Members.

160. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

161. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

162. And if a second breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class Members' injuries.

163. If an injunction is not issued, the resulting hardship to Plaintiff and Class Members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

164. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class Members, and the public at large.

PRAYER FOR RELIEF

Plaintiff and Class Members respectfully request judgment against Defendant and that the Court enter an order:

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

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

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

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

E. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: August 11, 2025.

Respectfully submitted,

By: /s/ Cristina Perez Hesano

PEREZ LAW GROUP, PLLC
7508 N. 59th Avenue
Glendale, AZ 85301
602-730-7100
cperez@perezlawgroup.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**Pro hac vice forthcoming*
Attorneys for Plaintiff and Proposed Class

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): **Steven Swinnerton , ;**

County of Residence: Maricopa

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Cristina Perez Hesano ,
Perez Law Group
7508 N. 59th Ave.
Glendale, Arizona 85301
602-730-7100
Samuel J. Strauss ,
Strauss Borrelli, PLLC
980 N. Michigan Ave., Ste 1610
Chicago, Illinois 60611
872-263-1100
Raina C. Borrelli ,
Strauss Borrelli, PLLC
980 N. Michigan Ave., Ste. 1610
Chicago, Illinois 60611
872-263-1100

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

County of Residence: Maricopa

Defendant's Atty(s):

,

,

IFP REQUESTED

REMOVAL FROM COUNTY, CASE #

II. Basis of Jurisdiction: **3. Federal Question (U.S. not a party)**

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

Plaintiff:- **N/A**

Defendant:- **N/A**

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

V. Nature of Suit: **380 Other Personal Property Damage**

VI.Cause of Action: **28 USC 1332**

VII. Requested in Complaint

Class Action: **Yes**

Dollar Demand:

Jury Demand: Yes

VIII. This case **is not related** to another case.

Signature: Cristina Perez Hesano

Date: 08/11/2026

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