UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF NEW YORK

EDWARD KOELLER, individually and on behalf of all others similarly situated, Plaintiff, v. NUMRICH GUN PARTS CORPORATION, Defendant.	Case No. **1:22-cv-675 (DNH/CFH)** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff, Edward Koeller ("Plaintiff"), files this Class Action Complaint on behalf of himself, and all others similarly situated against the Defendant, Numrich Gun Parts Corporation ("Numrich" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. On personal knowledge of his own circumstances and upon investigation and information and belief of his counsel, Plaintiff alleges the following:

INTRODUCTION

1. Numrich, a firearms parts retailer, lost control over at least 45,169 of its e-commerce customers' highly sensitive personal and financial information in a data breach by cybercriminals ("Data Breach").

2. On or around March 28, 2022, Numrich became aware of suspicious activity on its e-commerce website, www.gunpartscorp.com. Numrich's investigations revealed that hackers gained unauthorized access to customers' confidential personal information and their payment card data (together "PCD"). The Data Breach occurred between January 23, 2022, and April 5, 2022

(the "Breach Period").

3. On information and belief, hackers gained unauthorized access to Numrich customers' PCD who made purchases through the website during the Breach Period.

4. Numrich electronically collects and stores its online customers' payment card information after each purchase—withholding within its systems a treasure trove of useful information attractive for hackers who can use the payment data to make fraudulent purchases and cause real substantial damage to consumers.

5. On information and belief, Numrich placed its personal financial gains ahead of its customers' interests and refused to shut down e-commerce through its website, even after discovering the Data Breach and prior to providing any type of notice about the breach.

6. On information and belief, the stolen PCD included, at least, customers' names, addresses, payment card numbers, card security codes, and expiration dates.

7. On information and belief, cybercriminals were able to breach Numrich's website and system because Numrich did not maintain reasonable security safeguards or protocols to protect its customers' PCD, leaving it an unguarded target for theft and misuse.

8. On information and belief, the Data Breach was undetected for over two months.

9. On or around June 6, 2022—over two months after discovering the breach and nearly five months after the start of the breach—Numrich began to notify breach victims that their PCD was compromised (the "Breach Notice").

10. When Numrich finally announced the Data Breach, it deliberately underplayed the breach's severity and misrepresented that it was "unaware of any actual misuse of information related to [the breach,]" even though Numrich knew cybercriminals had infiltrated its website and data for months. Numrich's Breach Notice obfuscated the nature of the breach and the threat it

posed—refusing to tell its customers how many people were impacted, how the breach happened, or why it took over two months for Numrich to send a bare-bones notice. A true and correct copy of the Breach Notice is attached hereto as **Exhibit A**.[1]

11. Numrich's failure to safeguard customers' PCD and adequately warn them about the Data Breach violates New York and Missouri law, harming thousands of individuals. Plaintiff Koeller received Numrich's Breach Notice and is a Data Breach victim, causing him to seek relief on a class wide basis.

12. Numrich knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of the breach.

13. Numrich's misconduct has injured the Plaintiff and members of the proposed Class, including: (i) costs associated with the prevention, detection, and recovery from fraudulent charges, and other unauthorized use of their data; (ii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iii) emotional distress associated with the loss of control over their PCD.

14. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate data security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PCD. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

15. On information and belief, the customer information and PCD compromised in the Data Breach is still stored in Numrich's online systems, Plaintiff and members of the proposed

[1] Breach Notice obtained from the website of the office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/c85b1a09-ea9b-4402-abb0-4d404f02d730.shtml (last visited June 15, 2022).

Class have an interest in ensuring that their information is safe, and they should be entitled to seek injunctive and other equitable relief, including independent oversight of Numrich's security system.

16. Plaintiff and members of the proposed Class therefore bring this lawsuit seeking damages and relief for Defendant's actions.

PARTIES

17. Plaintiff, Edward Koeller, is a natural person and adult citizen of Missouri. Mr. Koeller intends to remain domiciled in Missouri indefinitely, and maintains his true, fixed, and permanent home in Missouri. Mr. Koeller has been a Numrich customer since September 2015 and Data Breach victim, receiving Numrich's Breach Notice in June 2022.

18. Defendant, Numrich Gun Parts Corporation, is a New York Corporation, with its principal place of business at 226 Williams Lane, Kingston, NY, 12401.

JURISDICTION & VENUE

19. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant, establishing minimal diversity.

20. This Court has personal jurisdiction over Defendant because it is incorporated in New York and its corporate headquarters is in Kingston, New York.

21. Venue is proper in this Court under 28 U.S.C.§ 1391 because a substantial part of the alleged wrongful conduct and events giving rise to the claims occurred in this District and because Defendant conducts significant business in this District.

BACKGROUND FACTS

a. Numrich's Failure to Prevent the Data Breach

22. Plaintiff and members of the proposed Class are Numrich's former and current online customers.

23. To complete online transactions, Numrich requires its customers to enter their payment card and personal information in order to receive the firearms parts being purchased.

24. When Numrich collects this sensitive information, it promises to use reasonable measures to safeguard the PCD from theft and misuse.

25. In fact, Numrich informs its online customers that it collects and maintains their PCD through the Privacy Policy (the "Privacy Policy").[2] A true and correct copy of the Privacy Policy is attached hereto as **Exhibit B**.

26. The Privacy Policy warrants that the privacy of its customers is "important" to Numrich. Indeed, Numrich asserts that it "does not sell, trade, or share [customers'] information with anybody," and that Numrich "is a highly ethical company and requires the highest standard of conduct from [its] employees and business partners." Exh. B.

27. Numrich represented to its online customers that their PCD would be secure. Plaintiff and members of the proposed Class relied on such representations when they agreed to provide their PCD and transact with Numrich.

28. Consumers place value in data privacy and security. These are important considerations when deciding where to make certain purchases. Plaintiff would not have transacted with, nor provided his PCD to Numrich had he known that Numrich does not take all necessary precautions to secure the personal and financial data given to it by consumers.

[2] See Numrich's Website: https://www.gunpartscorp.com/privacy (last visited June 15, 2022).

29. Despite its alleged commitments to securing sensitive customer data, Numrich does not follow industry standard practices in securing customers' PCD.

30. In January 2022, hackers bypassed Numrich's security safeguards and infiltrated its systems, giving them unfettered access to customers' PCD.

31. On information and belief, the Data Breach was undetected for at least 2 months.

32. In response to the Data Breach, Numrich contends that it "took steps to confirm the security of [its] systems . . . [and] worked quickly to secure [its] website and implement additional network and endpoint monitoring to reduce the risk of recurrence." Exh. A. These measures should have been in place *before* the Data Breach.

33. Numrich's Breach Notice omits the size and scope of the breach. Numrich has demonstrated a pattern of providing inadequate notices and disclosures about the Data Breach.

34. On information and belief, the Data Breach has impacted at least 45,169 former and current Numrich online customers.

35. On information and belief, Numrich does not adequately train its employees on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems.

36. Numrich's negligent conduct caused the Data Breach. Numrich violated its obligation to implement best practices and comply with industry standards concerning website system security. Numrich failed to comply with security standards and allowed its customers' PCD to be accessed and stolen by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach.

37. On information and belief, Numrich did not cease its online operations during the Breach Period and exposed the PCD of additional customers after discovering the Data Breach.

b. Plaintiff's Experience

38. Plaintiff has been a Numrich customer since approximately 2015, making at least two purchases from Numrich's website, the most recent being on February 8, 2022.

39. As a condition of completing his online transactions, Plaintiff was required to provide his PCD to Numrich.

40. Plaintiff provided his PCD to Numrich and trusted that the company would use reasonable measures to protect it according to Numrich's Privacy Policy and state and federal law.

41. In mid-June 2022, Plaintiff received a notice letter from Numrich closely resembling the Breach Notice confirming Plaintiff's PCD was stolen as a result of the Data Breach.

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

c. Plaintiff and the Proposed Class Suffered Damages

43. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PCD that can be directly traced to Defendant.

44. According to a 2020 Federal Trade Commission report, credit card fraud is the most common type of identity theft.[3]

45. As a result of Numrich's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost

[3]https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf (last visited June 15, 2022).

time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PCD is used;

b. The diminution in value of their PCD;

c. The compromise and continuing publication of their PCD;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Unauthorized use of stolen PCD; and

g. The continued risk to their PCD, which remains in the possession of defendant and is subject to further breaches so long as defendant fails to undertake the appropriate measures to protect the PCD in their possession.

46. Stolen credit cards are considered highly valuable commodities on the criminal information black market. According to Forbes Advisor, a team of financial and economy journalists, a single consumer's stolen credit card information can be worth up to $150.00 depending on the type of supplementary information included.[4] Indeed, selling stolen credit card information in "bulk guarantees a lucrative payout—even if the fraud does not ultimately

[4] *What Happens to Stolen Credit Card Numbers?*, Forbes.com (Apr. 19, 2022), https://www.forbes.com/advisor/credit-cards/what-happens-to-stolen-credit-card-numbers/#:~:text=A%20single%20consumer's%20stolen%20credit%20information%20card%20sells,value%20of%20the%20card%2C%20but%20not%20by%20much (last visited June 15, 2022).

succeed."[5]

47. Payment card data breaches can have devastating and lasting impacts on breach victims. Criminals learn the victims' purchasing behaviors and habits, and can use this sensitive information to mimic the victims' behaviors to lower the chances of fraudulent charges getting caught by financial institutions and the breach victims themselves.[6]

48. It can take victims months or years to spot identity or PCD theft, giving criminals plenty of time to use that information for cash.

49. Criminals in possession of stolen credit card information can take over the victims' existing accounts, make fraudulent charges, and even open new accounts using the victims' personal financial information without their knowledge.[7]

50. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff and other members of the proposed Class's stolen PCD is being misused, and that such misuse is fairly traceable to the Data Breach.

51. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, leading to more than $3.5 billion in losses to individuals and business victims.[8]

52. Further, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[9] Defendant did not rapidly report to Plaintiff and the

---

[5] *Id.*
[6] *Id.*
[7] *15 Disturbing Credit Card Fraud Statistics*, Cardrates.com (Mar. 16, 2022), https:// www.cardrates.com/advice/credit-card-fraud-statistics/ (last visited June 15, 2022).
[8] *2019 Internet Crime Report Release*, fbi.gov (Feb. 11, 2020), https:// www.fbi.gov/news/stories/2019-internet-crime-report-released-021120#:~:text=The%20Importance%20of%20Reporting,-"Information%20reported%20to&text=Rapid%20reporting%20can%20help%20law,to%20build%20on%20its%20success. (last visited June 15, 2022).
[9] *Id.*

Class that their PCD had been stolen.

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

54. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PCD. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

55. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PCD. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years to come.

56. Defendant disclosed the PCD of Plaintiff and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PCD of Plaintiff and members of the proposed Class 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 PCD.

57. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PCD of Plaintiff and potentially thousands of members of the proposed Class to unscrupulous

operators, con artists and outright criminals.

58. Defendant's failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff and members of the proposed Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PCD and take other necessary steps to mitigate the harm caused by the Data Breach.

CLASS ACTION ALLEGATIONS

59. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and all members of the proposed class (the "Class"), defined as follows:

> All persons in the United States whose personal and financial information was compromised in the Data Breach disclosed by Numrich in June 2022.

60. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons

61. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

62. This action satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

a. **Numerosity**. Plaintiff is representative of the proposed Class, consisting of thousands of members, far too many to join in a single action;

b. **Ascertainability**. Class members are readily identifiable from information in Defendant's possession, custody, and control;

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

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. Plaintiff's interests do not conflict with Class members' interests and Plaintiff has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel. Defendant has no defenses unique to Plaintiff.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for all Class members. Common questions for the Class include, but are not necessarily limited to the following:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff and the Class's PCD;

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

iii. Whether Defendant was negligent in maintaining, protecting, and securing PCD;

iv. Whether Defendant breached contract promises to safeguard Plaintiff and the Class's PCD;

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

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff and the Class injuries;

viii. What the proper damages measure is; and

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

63. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

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

64. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

65. Plaintiff and members of the Class entrusted their PCD to Defendant. Upon accepting and storing Plaintiff's and members of the Class's PCD in its database system, Defendant undertook and owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PCD in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at

unauthorized access.

66. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PCD in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PCD —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PCD by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PCD was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

67. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PCD. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PCD, 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.

68. Defendant owed these duties to Plaintiff and members of the Class 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 protocols. Defendant actively sought and obtained Plaintiff's and members of the Class's personal information and PCD.

69. The risk that unauthorized persons would attempt to gain access to the PCD and misuse it was foreseeable. Given that Defendant holds vast amounts of PCD, it was inevitable that

unauthorized individuals would attempt to access Defendant's databases containing the PCD — whether by malware or otherwise.

70. PCD is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PCD of Plaintiff and members of the Class's and the importance of exercising reasonable care in handling it.

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

72. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including, but not limited to: monetary damages arising from unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the stolen PCD and/or filing false tax returns; damages from identity theft, which may take months, if not years, to discover and detect, given the far-reaching, adverse, and detrimental consequences of identity theft and loss of privacy; and embarrassment, humiliation, frustration, and emotional distress. The nature of other forms of economic damage and injury may take years to detect and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft of PCD described above.

COUNT II
Breach of Implied Contract

(On Behalf of Plaintiff and the Class)

73. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

74. Defendant solicited Plaintiff and members of the Class to purchase firearms parts through its website using their credit or debit cards. Plaintiff and members of the Class accepted Defendant's offers and used their credit or debit cards to purchase goods from Defendant's website during the period of the Data Breach.

75. When Plaintiff and members of the Class made and paid for purchases, they provided their PCD by entering their credit or debit card numbers/information into the Defendant's website. In doing so, Plaintiff and members of the Class entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and members of the Class if their data had been breached and compromised.

76. Each purchase on the Defendant's website during the Data Breach period was made pursuant to the mutually agreed-upon implied contract with Defendant under which Defendant agreed to safeguard and protect Plaintiff's and members of the Class's PCD and to timely and accurately notify Plaintiff and members of the Class if such information was compromised or stolen.

77. Plaintiff and the members of the Class would not have provided and entrusted their PCD to Defendant to make purchases through the website in the absence of the implied contract between them and Numrich.

78. Defendant materially breached the contract(s) it had entered with Plaintiff and members of the Class by failing to safeguard and protect the PCD and by failing to notify Plaintiff

and members of the Class promptly of the intrusion into its website system that compromised such information. Defendant further breached the implied contracts with Plaintiff and members of the Class by:

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

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

c. Failing to ensure the confidentiality and integrity of electronic PCD that Defendant created, received, maintained, and transmitted.

79. The damages sustained by Plaintiff and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

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

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

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

83. Defendant failed to advise Plaintiff and members of the Class of the Data Breach promptly and sufficiently.

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

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

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

86. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

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

88. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of payments through Defendant's website.

89. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiff and members of the Class. Defendant also benefited from the receipt of Plaintiff and members of the Class's PCD, as this was used to facilitate their purchases.

90. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's payments and their PCD because Defendant failed to adequately protect their PCD. Plaintiff and the proposed Class would not have provided their PCD had they known Defendant would not adequately protect their PCD.

91. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of

its misconduct and Data Breach.

COUNT IV
Violation of the New York General Business Law, N.Y. Gen. Bus. Law § 349 *et seq.*
(On Behalf of Plaintiff and the Class)

92. Plaintiff and members of the Class incorporate all previous paragraphs as if fully set forth herein.

93. New York General Business Law § 349 ("GBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in the state of New York.

94. As a well-known firearm parts retailer, Numrich conducted business, trade, or commerce in New York State.

95. In the conduct of its business, trade and commerce, and in furnishing retail services in New York State, Numrich's actions were directed at consumers.

96. In the conduct of its business, trade and commerce, and in furnishing retail services in New York State, Numrich collected and stored highly personal and private financial information, including PCD belonging to Plaintiff and members of the Class.

97. In the conduct of its business, trade and commerce, and in furnishing retail services in New York State, Numrich engaged in deceptive, unfair, and unlawful trade acts or practices, in violation of GBL § 349, including but not limited to the following:

a. Numrich misrepresented and fraudulently advertised material facts, pertaining to the sale and/or trading of firearms parts to Plaintiff and the members of the Class that it would maintain adequate data privacy and security practices and procedures to safeguard its E-commerce customers' PCD from unauthorized sharing, disclosure, release, sell, or trade, and moreover, that its employees and business

partners would do the same;

b. Numrich misrepresented material facts, pertaining to the sale and/or trading of firearm parts, to **Plaintiff and** the members of the proposed Class by representing and advertising that it did and would comply with requirements of relevant federal and state laws pertaining to privacy and security of its E-commerce customers' PCD, and that its employees and business partners would do the same;

c. Numrich omitted, suppressed, and concealed the material facts of the Data Breach and its privacy and security protections for its E-commerce customers' PCD during the Breach Period—even after discovering the Data Breach;

d. Numrich engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of the Class's PCD, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the Data Breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15. U.S.C. § 45);

e. Numrich engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the Data Breach to the Plaintiff and members of the proposed Class "in the most expedient time possible and without unreasonable delay," contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2); and

f. Numrich engaged in deceptive, unfair, and unlawful trade acts or practices by failing to take proper action following the Data Breach to enact adequate privacy and security measures to protect the Class's PCD from further unauthorized disclosure, release, data breaches, and theft.

98. Numrich systematically engaged in these deceptive, misleading, and unlawful acts

and practices, to the detriment of the Plaintiff and members of the proposed Class.

99. Numrich willfully engaged in such acts and practices, and knew it violated GBL § 349 or showed reckless disregard for whether it violated GBL § 349.

100. As a direct and proximate result of Numrich's deceptive trade practices, the Plaintiff and members of the proposed Class suffered injury and/or damages, including the loss of their legally protected interest in the confidentiality and privacy of their PCD, and the loss of the benefit of their respective bargains.

101. The above unfair deceptive practices and acts committed by Numrich were unscrupulous, unethical, immoral, and oppressive. These acts caused substantial injury to Numrich's E-commerce customers that these consumers could not reasonably avoid. The substantial injuries outweighed any benefits to Numrich's E-commerce customers or to competition.

102. Numrich knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiff's and members of the proposed Class's PCD and that risk of a data breach or cyber-attack were highly likely and foreseeable. Numrich's actions in engaging in the above-referenced unfair practices and deceptive acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of the Plaintiff and members of the proposed Class.

103. Plaintiff and members of the Class seek relief under GBL § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request 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 is necessary to protect the interests of Plaintiff and the Class;

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

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen PCD;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

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

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

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

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

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: June 24, 2022

Respectfully submitted,

By: */s/ James J. Bilsborrow*

James J. Bilsborrow (Bar Roll # 519903)
jbilsborrow@weitzlux.com
WEITZ & LUXENBERG, PC
700 Broadway
New York, New York 10003
Telephone: (212) 558-5500

Samuel J. Strauss*
sam@turkestrauss.com
Raina C. Borrelli*
raina@turkestrauss.com
Alex Phillips*
alexp@turkestrauss.com
TURKE & STRAUSS LLP
613 Williamson St., Suite 201
Madison, WI 53703
Telephone (608) 237-1775

**pro hac vice* forthcoming

Attorneys for Plaintiff and the Proposed Class