UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

JOHN DOE, individually and on behalf of all others similarly situated, Plaintiff, v. LASTPASS US LP Defendant.	)	Case No.: JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Individually and on behalf of others similarly situated, Plaintiff John Doe brings this action against Defendant LastPass US LP ("LastPass"). Plaintiff's allegations are based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiff's attorneys. Plaintiff believes that substantial additional evidentiary support for the allegations set forth herein exists and will be revealed after a reasonable opportunity for discovery.

I. INTRODUCTION

1. This is a class action for damages against Defendant for its failure to exercise reasonable care in securing and safeguarding highly sensitive consumer data in connection with a massive, months-long data breach that began in August 2022 (the "Data Breach") and impacted the highly sensitive data of potentially millions of LastPass users, including Plaintiff and putative Class (defined below) members, resulting in the unauthorized public release and subsequent misuse of their names, end-user names, billing addresses, email addresses, telephone numbers, IP addresses from which customers were accessing the LastPass service, and customer vault data

where certain unencrypted data was stored, including website usernames and passwords, secure notes, and form-filled data (collectively, the "Private Information").

2. LastPass is a global password and identity management solutions company used by more than 30 million users and 85,000 businesses worldwide.

3. To the world of cybercriminals, LastPass users' Private Information, including the vault data that was in LastPass's possession at the time of the Data Breach, is extremely valuable. By accessing Plaintiff's and Class members' Private Information, hackers can simply unlock the stolen vaults using the victims' respective master passwords, which were likely stored by LastPass and ultimately accessed by the bad actors and wreak financial havoc on the lives of LastPass users like Plaintiff.

4. The security of LastPass customers' Private Information is, therefore, of the utmost importance. LastPass understood and appreciated the value of this Information yet chose to ignore it by failing to invest in adequate data security measures that would protect Plaintiff and the Class from the unauthorized access to, and copying of, their Private Information.

5. With their Private Information now in the hands of cybercriminals looking to profit from the theft, Plaintiff's and Class members' Private Information is no longer secure and has already been fraudulently misused, causing Plaintiff and members of the Class to suffer (and continue to suffer) economic and non-economic harms, as well as a substantial and imminent risk of future economic and non-economic harms.

6. LastPass understands the serious nature of data breaches and the potential theft and misuse of customers' highly sensitive information resulting therefrom, and purports to address these issues. In fact, LastPass acknowledges on its website that "[d]ata breaches are on

the rise," and that "[d]oing nothing could mean losing everything."[1] LastPass also touts that "[a]s a pioneer in cloud security technology, [it] provides award-winning password and identity management solutions that are convenient, effortless, and easy to manage," and that it "values users' privacy and security, so [their] sensitive information is always hidden[.]"[2]

7. However, even with this knowledge, LastPass's lax data security measures led to the Data Breach and, as a result, Plaintiff and Class members are no longer in possession of a secure customer vault. Their Private Information is no longer hidden but is, instead, in the hands of cybercriminals who have already fraudulently misused such data.

8. While the exact reason(s) for the Data Breach remain unclear, there is no doubt that Defendant failed to adequately protect Plaintiff's and Class members' Private Information and incorporate the tools necessary to keep such Private Information safe; such negligent failures resulted in the injuries alleged herein.

9. Had Plaintiff and the Class known that the Private Information they entrusted to Defendant in exchange for the services offered would not be adequately protected, they would not have entrusted their valuable Private Information to Defendant in order to use its product.

10. Thus, on behalf of the Class of victims also impacted by the Data Breach described herein, Plaintiff seeks, under state common law and consumer protection statutes, to redress Defendant's misconduct.

II. PARTIES

A. Plaintiff John Doe

11. Plaintiff Doe signed up to use LastPass in or around early May of 2016. In making the decision to entrust his Private Information to LastPass, Plaintiff relied upon the data

[1] *See* https://www.lastpass.com/company/about-us (last accessed December 29, 2022).
[2] *See id*. (last accessed December 29, 2022).

security services and privacy guarantees advertised by Defendant. Plaintiff Doe is a citizen and resident of Pennsylvania.

12. Beginning in or around early July 2022, Plaintiff began purchasing Bitcoin incrementally over the course of three months. The total dollar amount of these purchases was roughly $53,000.00. At the time of his first Bitcoin purchase, and despite never knowing of any requirements by Defendant to do so, Plaintiff updated his master password to more than 12 characters using a password generator, thus complying with Defendant's "best practices," so that he could store the highly sensitive private keys associated with his Bitcoin purchases in his LastPass customer vault.

13. However, Plaintiff's LastPass default settings only allowed for up to 100,100 password iterations.

14. Upon learning of the Data Breach, Plaintiff deleted his Private Information from his customer vault. However, on or around Thanksgiving weekend of 2022, Plaintiff's Bitcoin was stolen using the private keys he stored with Defendant. Plaintiff discovered the theft a week later and called the police, filed a police report, and filed a report with the FBI through the Internet Crime Complaint Center ("IC3.gov") but has not yet heard from these authorities.

15. Plaintiff is very careful about sharing his highly sensitive Private Information. He has never knowingly transmitted unencrypted sensitive personally identifiable information or information that is otherwise confidential over any unsecured source. He stores any documents containing his sensitive personal information in a safe and secure location or destroys the documents, and diligently chooses unique usernames and uses password generators for his various online accounts, all of which are stored on LastPass. Even so, the LastPass Data Breach has, through no fault of his own, exposed him to the theft of his Bitcoin and exposed him to

continued risk.

16. Plaintiff would not have given LastPass his Private Information had he known that the sensitive information collected by LastPass would be at risk of compromise and misuse due to Defendant's negligent data security practices.

17. Plaintiff has suffered the damages described herein, including but not limited to, the fraudulent removal of cryptocurrency from his portfolio due to the compromise of his Private Information, and remains at a significant risk of additional attacks now that his Private Information has been stolen In addition, Plaintiff and Class members have also been harmed as follows: the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value between the services *with* adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to change multiple account passwords, the master password, monitor accounts, and file police reports and reports with the FBI. Additionally, Plaintiff and Class members have been put at increased, substantial risk of future fraud and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

E. Defendant LastPass

18. Defendant LastPass is a limited partnership organized under the laws of Delaware, with its principal place of business in Boston, Massachusetts. LastPass, as a password and identity management services company, had access to its users' Private Information and failed to secure the received Private Information or implement any data security measures sufficient to ensure that the highly sensitive customer data that it stored would be securely handled.

JURISDICTION AND VENUE

19. Jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) because the matter in controversy exceeds the value of $5,000,000, exclusive of interests and costs, there are more than 100 class members, and the matter is a class action in which any member of a class of plaintiffs is a citizen of a different state from any defendant.

20. This Court has personal jurisdiction over this action because Defendant is headquartered in Massachusetts and has thus availed itself of the rights and benefits of the Commonwealth of Massachusetts by engaging in activities including (i) directly and/or through its parent company, affiliates and/or agents providing services throughout the United States and in this judicial district and abroad; (ii) conducting substantial business in this forum; (iii) having a registered agent to accept service of process in the Commonwealth of Massachusetts; and/or (iv) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in Massachusetts and in this judicial District.

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant resides within this District and has purposefully engaged in activities, including transacting business in this District and engaging in the acts and omissions alleged herein, in this District.

FACTUAL ALLEGATIONS

A. LastPass "Best Practices" Were Woefully Insufficient to Protect its Users' Private Information from Compromise and Misuse

22. LastPass allows customers to store, control and monitor highly sensitive account passwords, cryptocurrency keys, and other personal account information in their customer vaults, promising to "work[] tirelessly to advance the world of digital security[,]" and "improv[e] the LastPass tools [its] customers know and love to ensur[e] that [its customers'] data belongs only

to [them]."[3]

23. Customers use their vaults to store their Private Information in a safe and encrypted environment so as to protect such Information from unauthorized use, which unauthorized use would lead to the access and misuse of user passwords, cryptocurrency keys, and other personal account information stored in the customer vaults.

24. The LastPass customer vaults are themselves secured with a master password. LastPass claims in its blog post notice that these master passwords were not among the Private Information accessed in the Data Breach, and that they could not have been accessed in the Breach because "the master password is never known to LastPass and is not stored or maintained by LastPass."[4] Not only has this statement not been verified through discovery, but it is also a shameless attempt by LastPass to shift the blame of the Data Breach's resulting negative impact on Plaintiff and Class members by stating that "it would be extremely difficult to attempt to brute force guess master passwords for those customers who follow our password best practices."[5]

25. However, Defendant never provided direct notice to Plaintiff or Class members of any such "best practices," nor did it ever attempt to enforce these practices; not to mention, Defendant's "stronger-than-typical" implementation of 100,100 iterations of the PBKDF2 algorithm is actually well below the standard 310,000 iterations recommendation by the Open Web Application Security Project ("OWASP").[6]

26. Defendant's own notice also fails to rule out the possibility of credential stuffing and brute force attacks against Plaintiff's and Class members' vaults in order to access the

[3] *See* https://www.lastpass.com/company/about-us (last accessed December 29, 2022).
[4] *See* https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed December 29, 2022).
[5] *See id*.
[6] *See* https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html#pbkdf2 (last accessed December 29, 2022).

Private Information, attacks which would not be possible but for the LastPass Data Breach. And while LastPass attempts to persuade LastPass users that the twelve-character minimum for master passwords "greatly minimizes the ability for successful brute force password guessing," and that "it would take millions of years to guess your master password using generally-available password-cracking technology," modern graphics cards used at guessing PBKDF2-protected passwords are "becoming much better at guessing" and that some twelve-character passwords "could be guessed in slightly more than two months on the same graphics card."[7] Indeed, as pointed out by Mitchell Clark of the Verge (a technology-focused news site), "It goes without saying that a motivated actor trying to crack into a specific target's vault could probably throw more than one [graphic processor ("GPU")] at the problem, potentially cutting that time down by orders of magnitude."[8]

27. Furthermore, because the attackers were also able to compromise websites as a result of the Breach, they can target specific people who have specific accounts – for example, they could target users, like Plaintiff, who have purchased cryptocurrency, making their efforts to break into specifically targeted vaults much more efficient and less time consuming.

28. Many password managers have solved this issue by either adding a truly random factor to the encryption – a secret key – or by switching to key generation methods that are much more difficult to brute force than PBKDF2.[9] Others that similarly use only roughly 100,000 password iterations will also add another 100,000 iterations when their users' respective master passwords are stored on the company's server, thereby totaling roughly 200,000 iterations.[10]

---

[7] *See* https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/ (last accessed December 29, 2022).
[8] *See* https://www.theverge.com/2022/12/28/23529547/lastpass-vault-breach-disclosure-encryption-cybersecurity-rebuttal (last accessed December 29, 2022).
[9] *See id*.
[10] *See id*.

LastPass has implemented none of these best practices, yet now attempts to blame its customers for its very own data security failures that led to the Data Breach and resulting harms now suffered by Plaintiff and the Class.

B. The Data Breach

29. On August 25, 2022, LastPass issued the following notice:

> To All LastPass Customers,
>
> I want to inform you of a development that we feel is important for us to share with our LastPass business and consumer community.
>
> Two weeks ago, we detected some unusual activity within portions of the LastPass development environment. After initiating an immediate investigation, we have seen no evidence that this incident involved any access to customer data or encrypted password vaults.
>
> We have determined that an unauthorized party gained access to portions of the LastPass development environment through a single compromised developer account and took portions of source code and some proprietary LastPass technical information. Our products and services are operating normally.
>
> In response to the incident, we have deployed containment and mitigation measures, and engaged a leading cybersecurity and forensics firm. While our investigation is ongoing, we have achieved a state of containment, implemented additional enhanced security measures, and see no further evidence of unauthorized activity.
>
> Based on what we have learned and implemented, we are evaluating further mitigation techniques to strengthen our environment. We have included a brief FAQ below of what we anticipate will be the most pressing initial questions and concerns from you. We will continue to update you with the transparency you deserve.
>
> Thank you for your patience, understanding and support.
>
> Karim Toubba
>
> CEO LastPass

30. Then, on December 22, 2022, LastPass issued an updated notice announcing that

"an unknown threat actor accessed a cloud-based storage environment leveraging information obtained from the incident we previously disclosed in August of 2022."[11]

31. Upon information and belief, the Data Breach involved the data of millions of LastPass users. Hackers were able to copy highly sensitive information that included names, end-user names, billing addresses, email addresses, telephone numbers, IP addresses from which customers were accessing the LastPass service, and customer vault data where certain unencrypted data was stored, including website usernames and passwords, secure notes, and form-filled data.

32. During the delay between the initial August notice irresponsibly stating that users faced no significant risks and the December notice, the risks and damages to Plaintiff and Class members were only increasing. A prompt and proper response from Defendant, including full disclosure to all customers involved in the Data Breach of the extent of the Breach and the specific information impacted as a result of the Breach, as well as the risks users faced, would have mitigated those risks and resulting damages substantially, as users would have been able to change their impacted accounts' usernames and passwords, as well as their LastPass master passwords. Users also could have updated their default password iterations.

33. Thus, Defendant's disclosure, in addition to being unreasonably delayed, has been woefully inadequate and directly contributed to the damages suffered by Plaintiff and the Class thus far, and Defendant has yet to offer any remedy to assist Plaintiff and Class members through the devastating aftermath of its Breach. Instead, Defendant took months to "investigate" the ongoing Data Breach. Its investigation is *still* ongoing and may reveal even more egregious aspects of the Breach than those that have already been revealed, including, upon information

[11] https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed December 29, 2022).

and belief, that LastPass stored users' master password hashes with the usernames, thus allowing hackers to pull the full list of password hashes and start targeting and cracking specifically targeted master passwords.

34. Furthermore, the Data Breach exposed the physical addresses of the customers who lost their information in the Data Breach, meaning that users' home addresses will not be safe unless they change their addresses.

35. Defendant not only failed to adequately disclose the Data Breach to impacted customers, but it also failed to explain the extent of the Data Breach, where the information was lost, and to whom it may have been lost.

36. Users, cybersecurity experts, other password management companies, and the media have each justly criticized LastPass, in one instance stating that it is "abundantly clear that [LastPass does] not care about their own security, and much less about your security."[12]

C. LastPass Violated the FTC Act and Failed to Observe Reasonable and Adequate Data Security Measures

37. Defendant was prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "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. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

38. The FTC has promulgated numerous guides for businesses that highlight the

[12] *See The LastPass Disclosure of Leaked Password Vaults is Being Torn Apart by Security Experts* (Dec. 2022), https://www.theverge.com/2022/12/28/23529547/lastpass-vault-breach-disclosure-encryption-cybersecurity-rebuttal (last accessed December 29, 2022); *see also What's in a PR Statement: LastPass Breach Explained* (Dec. 2022), https://palant.info/2022/12/26/whats-in-a-pr-statement-lastpass-breach-explained/ (last accessed December 29, 2022).

importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[13]

39. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[14] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

40. The FTC further recommends that companies not maintain Private Information 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.[15]

41. 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 FTCA Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

42. Defendant was aware (or should have been aware), at all times, of its obligation to protect the Private Information of Plaintiff and Class members because of its position as

---

[13] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].
[14] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[15] *Start with Security*, *supra* note 32.

possessor and controller of such data. Defendant was also aware (or should have been aware as a password and identity management services company) of the significant repercussions that would result from its failure to do so.

43. Plaintiff and Class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligation to keep such information confidential and secure from unauthorized access.

44. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

45. Further, Defendant has been on notice for years that Plaintiff's and Class members' Private Information was a target for malicious actors due to, among other reasons, the high value to these bad actors of the Private Information stored in LastPass customers' vaults. Despite such knowledge, Defendant failed to implement and maintain reasonable and appropriate administrative and data security measures to protect Plaintiff's and Class members' Private Information from unauthorized access that Defendant should have anticipated and guarded against.[16]

46. Almost half of data breaches globally are caused by internal errors relating to either human mismanagement of sensitive information or system errors.[17] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[18] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the

[16] LastPass is not new to data breaches and security incidents; indeed, they are somewhat routine for LastPass, having previously occurred in 2011, 2015, 2016, 2017, 2019, 2020, and 2021. *See* https://en.wikipedia.org/wiki/LastPass.
[17] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.
[18] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.

risks of such errors.[19]

47. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[20]

48. To prevent and detect unauthorized access to its system, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply the latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privilege credentials;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

[19] *Id.*

[20] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[21]

49. These are basic, common-sense security measures that every business, not only those who handle sensitive information, should be taking. Defendant, with the highly sensitive personal information in its possession and control, should be doing even more. By adequately taking these common-sense solutions, Defendant could have prevented this Data Breach from occurring.

50. Charged with handling sensitive Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information that was entrusted to it and of the foreseeable consequences of a lapse in its data security. This includes the significant costs that would be imposed on Defendant's users because of a breach. Defendant failed, however, to take adequate administrative cybersecurity measures to prevent the Data Breach from occurring.

51. The Private Information was maintained in a condition vulnerable to misuse. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiff's and Class members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

52. As evidenced by these failures by Defendant to comply with its legal obligations established by the FTC Act, as well as its failures to maintain the reasonable and adequate data security measures set forth herein, Defendant failed to properly safeguard Plaintiff's and Class members' Private Information, allowing hackers to access and subsequently misuse it.

[21] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

53. But for Defendant's unlawful conduct, hackers would not have accessed Plaintiff's and the putative Class members' Private Information. Defendant's unlawful conduct—including active attempts to conceal the Data Breach and minimize the extent of the Data Breach or damages and place the blame on LastPass users—has directly and proximately resulted in widespread attacks against Plaintiff and the Class.

54. In addition to these types of threats, Plaintiff's and Class members' home addresses are now in the hands of cybercriminals. The class as a whole is comprised of a group of people who are at an especially high risk of ransom threats and blackmail attempts considering the types of accounts and value of accounts that have now been compromised as a result of Defendant's negligent data security practices. But for Defendant's unlawful conduct, such criminals would not have access to the home or other postal or billing addresses of Plaintiff and the Class. This access has resulted in, at minimum, an invasion of Plaintiff's and the Class's privacy and can lead to even greater damages, including theft or violent physical attacks.

55. The actions described herein have resulted in emotional distress for Plaintiff and the Class. Plaintiff and the Class have lost all security and privacy over important account information, as well as their home addresses, names, and other contact information, in addition to the fact that they lost money resulting from the targeted attacks in the Data Breach.

56. Plaintiff and the Class are anxious and alert as they are at a substantial risk of being bombarded with phishing emails and other scams, in addition to the fraud they have already suffered. Plaintiff is also suffering from the mental and emotional distress associated with such insecurity and uncertainty caused by the Data Breach. Class members, in addition to financial loss, mental anguish, and risk of future harm, continue to suffer from stress and anxiety as a result of the Data Breach.

57. As long as Plaintiff's and Class members' Private Information is in the hands of cybercriminals, they will remain at substantial, imminent risk of continued misuse of their Private Information. Defendant has not offered any solutions to remedy the damages to Plaintiff and the Class – in fact, the notice given to Plaintiff and Class members remarkably states that "[t]here are no recommended actions that you need to take at this time."[22] Plaintiff and Class members remain at permanent risk unless they take on the significant time and expense to change all of the Private Information that was exposed.

Damages to Plaintiff and the Class

58. Plaintiff has suffered damages from the Data Breach as set forth herein.

59. If Defendant had disclosed the full extent of the Data Breach in August instead of waiting months to do so, Plaintiff and Class members would have been on heightened alert and changed their passwords, thus avoiding the thefts that ensued.

60. As to other forms of damages, Plaintiff's and Class members' Private Information has been compromised and they have lost significant time having to sort through and change several accounts and passwords, and in addition, Plaintiff and Class members have incurred the following types of damages: the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value between the services *with* adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, that required to change multiple account passwords, the master password, monitor accounts, and file police reports and reports with the FBI. Additionally, Plaintiff and Class members have been put at increased, substantial risk of future fraud and/or

[22] *See* https://blog.lastpass.com/2022/12/notice-of-recent-security-incident/ (last accessed December 29, 2022).

misuse of their Private Information, which may take years to manifest, discover, and detect.

61. The Data Breach has also exposed the billing addresses of Plaintiff and Class members, which inherently impacts their physical security.

62. Had Plaintiff been made aware of Defendant's lax data security practices, unwillingness to promptly and completely disclose data breaches such as this one, and failure to provide timely notice and mitigatory assistance, Plaintiff would not have agreed to allow his Private Information to be held by Defendant.

The Monetary Value of Privacy Protections and Private Information

63. The fact that Plaintiff's and Class members' Private Information was inadvertently disclosed to bad actors that should not have had access to it – and has already been fraudulently misused – demonstrates the monetary value of the Private Information.

64. At all relevant times, Defendant understood the Private Information it collects from its users is highly sensitive and of significant property value. Indeed, Defendant itself uses data value and data privacy as a selling point for its own products.[23]

65. Preservation of the confidentiality of Private Information is a valuable property right. The value of the Private Information is axiomatic, considering the value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences.

66. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[24]

[23] *See* https://www.lastpass.com/company/about-us ("Doing nothing [to prevent data breaches] could mean losing everything.") (last accessed December 30, 2022).
[24] *See, e.g.*, https://datacoup.com/ (last accessed December 30, 2022).

67. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. This transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property.

CLASS ALLEGATIONS

68. Plaintiff brings this Action as a class action pursuant to Fed. R. Civ. P. 23 and seeks certification of the following Nationwide Class (referred to herein as the "Class"):

> Nationwide Class: All persons whose personal information was accessed, compromised, copied, stolen, and/or exposed as a result of the LastPass Data Breach.

69. Excluded from the Class are Defendant, its officers and directors, and members of their immediate families or their legal representatives, heirs, successors or assigns and any entity in which Defendant has or had a controlling interest.

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

71. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. Upon information and belief, the Class numbers in the millions. Moreover, the Class is composed of an easily ascertainable set of LastPass users who were thus impacted by the Data Breach. The precise number of Class members can be further confirmed through discovery, which includes Defendant's records. The disposition of Plaintiff's and Class members' claims through a class action will benefit the parties and this Court.

72. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2)**

and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems and/or protocol prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems and/or protocol prior to and during the Data Breach were consistent with industry standards and best practices;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;
- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiff and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

73. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and other members of the Class. Similar or identical common law 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 predominate in this action.

74. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured and sustained similar monetary and economic injuries as a result of Defendant's uniform misconduct described herein and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

75. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent, he has retained counsel competent and experienced in complex class action litigation, and he will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and his counsel.

76. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** 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. Civ. P. 23 (b)(2).

77. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far

fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

78. Class certification is also appropriate under Rules 23(b)(1) and/or (b)(2) because:

- The prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications establishing incompatible standards of conduct for Defendant;

- The prosecution of separate actions by individual Class members would create a risk of adjudication that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or would substantially impair or impede their ability to protect their interests; and

- Defendant has acted and refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive relief with respect to the members of the Class as a whole.

79. Class certification is also appropriate because this Court can designate particular claims or issues for class-wide treatment and may designate multiple subclasses pursuant to Fed. R. Civ. P. 23(c)(4).

80. No unusual difficulties are likely to be encountered in the management of this action as a class action.

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class)

81. Plaintiff incorporates the preceding paragraphs as though fully set forth herein.

82. Upon Defendant's acceptance and storage of Plaintiff's and Class members' Private Information in its system, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that Information and to use

commercially reasonable methods to do so. Defendant knew that the Private Information was highly sensitive and confidential and should be protected as such.

83. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate data security practices.

84. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, and protecting Private Information in its possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices, including at least 310,000 password iterations as recommended by OWASP; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

85. Defendant also breached its duty to Plaintiff and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering its dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of compromise and misuse, which permitted malicious bad actors to gather Plaintiff's and Class members' Private Information and intentionally disclose it to others and/or misuse it without consent, resulting in the harms alleged herein.

86. Defendant knew, or should have known, of the risks inherent in collecting and storing Plaintiff's and Class members' Private Information and the importance of adequate data

security.

87. Defendant knew, or should have known, that its data systems and privacy protocols and procedures would not adequately safeguard Plaintiff's and Class members' Private Information.

88. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate computer systems, networks, and/or data security practices to safeguard Plaintiff's and Class members' Private Information.

89. Because Defendant knew that the theft of the highly sensitive data stored in its systems would damage millions of individuals and businesses, including Plaintiff and Class members, Defendant had a duty to implement sufficient privacy practices and procedures and adequately protect its data systems and the Private Information contained therein.

90. Defendant's duty of care to use reasonable data security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class members, which is recognized by laws and regulations, including but not limited to, common law. Defendant was in a position to ensure that its systems and protocols were sufficient to protect against the foreseeable risk of harm to Class members from the compromise of the data with which it was entrusted.

91. In addition, Defendant had a duty to employ reasonable data 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 data security measures to protect confidential data.

92. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described herein, but also because Defendant was

bound by industry standards to do more to protect the confidential data that was compromised as a result of the Data Breach.

93. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their Private Information. Defendant's misconduct included failing to (1) secure Plaintiff's and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent the Data Breach.

94. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;
- Failing to adequately monitor the security of its networks and systems;
- Allowing unauthorized access to Class members' Private Information;
- Failing to detect in a timely manner that Class members' Private Information had been compromised; and
- Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for fraud and other damages.

95. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate data security and protect Plaintiff's and Class members' Private Information from being foreseeably accessed, stolen, disseminated, and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' Private Information during the time it was within Defendant's possession

and control.

96. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to, failing to adequately protect the Private Information, and failing to provide Plaintiff and Class members with timely notice that their sensitive Private Information had been compromised.

97. Neither Plaintiff nor Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint. Any and all actions taken by Plaintiff and Class members which Defendant may argue contributed to the misuse of the compromised Private Information were reasonable under the circumstances.

98. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members suffered damages as alleged herein.

99. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; and (ii) submit to future bi-annual audits of those systems and monitoring procedures.

COUNT II
BREACH OF CONTRACT/BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
(On Behalf of the Nationwide Class)

100. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

101. Plaintiff and Class members entered into valid and enforceable express contracts with Defendant under which Plaintiff and Class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide password and identity management services that included the implementation of adequate data security standards, protocols, and procedures to ensure the protection of Plaintiff's and Class members' Private Information.

102. In every contract entered into between Plaintiff and Class members and Defendant, including those at issue here, there is an implied covenant of good faith and fair dealing obligating the parties to refrain from unfairly interfering with the rights of the other party or parties to receive the benefits of the contracts. This covenant of good faith and fair dealing is applicable here as Defendant was obligated to protect (and not interfere with) the privacy and protection of Plaintiff's and Class members' Private Information.

103. To the extent Defendant's obligation to protect Plaintiff's and Class members' Private Information was not explicit in those express contracts, the contracts also included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class members' Private Information, including in accordance with trade regulations, federal, state and local laws, and industry standards. No customer would have entered into these contracts with Defendant without the understanding that their Private Information would be safeguarded and protected; stated otherwise, data security was an essential term of the parties' express contracts.

104. Indeed, Section 4.2 of Defendant's Terms of Service for Personal Users states that LastPass "ha[s] implemented and maintain appropriate organizational, administrative, and technical safeguards designed to protect your Content against any unauthorized access, loss, misuse, or disclosure."

105. A meeting of the minds occurred, as Plaintiff and Class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

106. The protection of Plaintiff's and Class members' Private Information was a material aspect of Plaintiff's and Class members' contracts with Defendant.

107. Defendant's promises and representations described above relating to industry standards and Defendant's purported concern about its users' privacy rights are express terms of the contracts between Defendant and its customers, including Plaintiff and Class members. Defendant breached these promises by failing to comply with reasonable industry practices.

108. Plaintiff and Class members read, reviewed, and/or relied on statements made by or provided by Defendant and/or otherwise understood that Defendant would protect its customers' Private Information if that information were provided to Defendant.

109. Plaintiff and Class members fully performed their obligations under their contracts with Defendant; however, Defendant did not.

110. As a result of Defendant's breach of these terms, Plaintiff and Class members have suffered a variety of damages including but not limited to: the lost value of their privacy; not receiving the benefit of their bargain with Defendant; losing the difference in the value between the services *with* adequate data security that Defendant promised and the services actually received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to change multiple account passwords, the master password, monitor accounts, and file police reports and reports with the FBI. Additionally, Plaintiff and Class members have been put at increased risk of future fraud and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

111. Plaintiff and Class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

112. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

113. Plaintiff brings this claim alternatively to his claim for breach of contract.

114. Through its course of conduct, Defendant entered into implied contracts with Plaintiff and Class members for the provision of password and identity management services, as well as implied contracts for Defendant to implement data security practices adequate to safeguard and protect the privacy of Plaintiff's and Class members' Private Information.

115. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when he first began using Defendant's services in or around May of 2016.

116. The valid and enforceable implied contracts to provide password and identity management services that Plaintiff and Class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information entrusted to it.

117. When Plaintiff and Class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

118. Defendant solicited and invited Plaintiff and Class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class members accepted Defendant's offer and provided their Private Information to Defendant.

119. By 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.

120. Under these implied contracts, Defendant promised and was obligated to: (a) provide password and identity management services to Plaintiff and Class members; and (b) protect Plaintiff's and the Class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and members of the Class agreed to turn over their Private Information to Defendant.

121. Both the provision of password and identity management services and the protection of Plaintiff's and Class members' Private Information were material aspects of these implied contracts.

122. The implied contracts for the provision of password and identity management services, including but not limited to, the maintenance of the privacy of Plaintiff's and Class members' Private Information, are also acknowledged, memorialized, and embodied in Defendant's Terms of Service for personal users.

123. Defendant's express representations, including, but not limited to, the express representations found in its Terms of Service, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff and Class members, and to protect the privacy of Plaintiff's and Class members' Private Information.

124. Users of password management services value their privacy and the ability to keep their Private Information associated with obtaining such services. Plaintiff and Class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected; nor would they have entrusted their Private Information to Defendant in the absence of the implied promise by Defendant to monitor the Private

Information and to ensure that it adopted reasonable administrative and data security measures.

125. A meeting of the minds occurred, as Plaintiff and Class members agreed and provided their Private Information to Defendant in exchange for, among other things, both the provision of password management services and the protection of their Private Information.

126. Plaintiff and Class members performed their obligations under the contract when they turned over their Private Information to Defendant.

127. Defendant materially breached its contractual obligation to protect the nonpublic Private Information it gathered when the Private Information was compromised and subsequently misused as a result of the Data Breach.

128. Defendant materially breached the terms of these implied contracts, including, but not limited to, the terms stated in the relevant Terms of Service. Defendant did not maintain the privacy of Plaintiff's and Class members' Private Information as evidenced by its recent notices of the Data Breach posted on its blog. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and Class members' Private Information as set forth above.

129. The Data Breach was a reasonably foreseeable consequence of Defendant's data security failures in breach of these contracts.

130. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and Class members did not receive the full benefit of their bargain with Defendant, and instead received services that were of a diminished value to that described in the contracts. Plaintiff and Class members therefore were damaged in an amount at least equal to the difference in the value of the password management accounts *with* data security protection that Defendant agreed to provide and the services Defendant actually provided.

131. Had Defendant disclosed that its administrative and data security measures were inadequate or that it did not adhere to industry-standard security measures, neither Plaintiff, Class members, nor any reasonable person would have utilized services from Defendant.

132. As a direct and proximate result of the Data Breach, Plaintiff and Class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation, the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they struck with Defendant.

133. Plaintiff and Class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

134. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.,* strengthen its data security systems and monitoring procedures, and immediately provide adequate credit monitoring to all Class members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

135. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

136. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from Defendant the services that were the subject of the transaction and were entitled to have Defendant protect their Private Information with adequate data security.

137. Defendant knew and appreciated that Plaintiff and Class members conferred a benefit on it and accepted and retained that benefit. Defendant profited from Plaintiff's and Class members' providing their Private Information to it for business purposes.

138. Defendant failed to secure Plaintiff's and Class members' Private Information and, therefore, did not provide full compensation for the benefit that Plaintiff's and Class members' Private Information provided.

139. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate security practices alleged herein.

140. If Plaintiff and Class members knew that Defendant did not have data security safeguards in place that were adequate to secure their Private Information from unauthorized access, they would not have used Defendant's services.

141. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class members conferred upon it.

142. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds in the amount of the benefits that it unjustly received from them by way of possessing and controlling Plaintiff's and Class members' Private Information.

143. This claim is being asserted in the alternative to Plaintiff's claims for breach of contract.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of the Nationwide Class)

144. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

145. Plaintiff and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendant and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

146. Defendant, in taking possession of this highly sensitive information, has a special relationship with its customers, including Plaintiff and the Class. As a result of that special relationship, Defendant was provided with and stored private and valuable information belonging to Plaintiff and the Class, which Defendant was required by law and industry standards to maintain in confidence.

147. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became a guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and Class Members, for the safeguarding of Plaintiff's and Class Members' Private Information.

148. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of this relationship, in particular, to keep secure Plaintiff's and Class members' Private Information and to maintain the confidentiality of their Private Information.

149. Defendant owed a duty to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

150. Plaintiff and Class members have a privacy interest in their personal and

proprietary matters and Defendant had a duty not to disclose such confidential information.

151. Plaintiff's and Class members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

152. Defendant breached its fiduciary duty to Plaintiff and Class members when Plaintiff's and Class members' Private Information was disclosed to unknown criminal hackers by way of Defendant's own acts and omissions, as alleged herein.

153. Defendant knowingly breached its fiduciary duties by failing to safeguard Plaintiff's and Class members' Private Information, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiff and Class members thereof; (g) failing to follow its own privacy policies and practices published to its customers; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiff's and Class members' Private Information to a criminal third party.

154. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

155. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered or will suffer injuries, including but not limited to, the following: loss of their privacy and confidentiality of their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendant's Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their Private Information.

156. Defendant breached its fiduciary duty to Plaintiff and Class members when it

made an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendant to retain the benefits it has received at Plaintiff's and Class members' expense.

157. Plaintiff and Class members are entitled to damages and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT VI
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(On Behalf of the Nationwide Class)

158. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

159. 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. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

160. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective duties to reasonably safeguard users' Private Information and whether LastPass is maintaining data security measures adequate to protect the Class members, including Plaintiff, from further data breaches that compromise their Private Information, including but not limited to, their respective customer vaults.

161. Plaintiff alleges that Defendant's data-security measures remain inadequate. Defendant denies these allegations and goes so far as to attempt to cast the blame of the harm suffered by Plaintiff and Class members upon Plaintiff and Class members themselves. In addition, Plaintiff and the Class continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private

Information and continued fraudulent activity against them will occur in the future.

162. Pursuant to its authority under the Declaratory Judgment Act, Plaintiff asks the Court to enter a judgment declaring, among other things, the following: (i) LastPass owes a duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and (ii) LastPass is in breach of these legal duties by failing to employ reasonable measures to secure consumers' Private Information in its possession and control.

163. Plaintiff further asks the Court to issue corresponding prospective injunctive relief requiring LastPass to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information from future data breaches.

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

165. The hardship to the Class members if an injunction does not issue exceeds the hardship to LastPass if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of LastPass, the Class members will likely be subjected to substantial hacking and phishing attempts and other damage, in addition to the damages already suffered. On the other hand, the cost to LastPass of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and LastPass has pre-existing legal obligations to employ such measures.

166. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches at LastPass, thus eliminating the additional injuries that would result to the Class members and the millions of consumers whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class proposed in this Complaint, respectfully requests that the Court enter judgment in favor of Plaintiff and the Class and against Defendant, as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to LastPass's lax data security practices, procedures, networks, and systems that led to the unauthorized disclosure and subsequent misuse of Plaintiff's and Class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity all types of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the benefits wrongfully retained by Defendant as a result of its wrongful conduct;

E. For an award of damages, compensatory damages and/or restitution or disgorgement, in an amount to be determined, as allowable by law;

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

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

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

JURY DEMAND

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

Dated: January 3, 2023

Respectfully submitted,

/s/ David Pastor
BBO #391000
PASTOR LAW OFFICE, PC
63 Atlantic Avenue, 3rd Floor
Boston, MA 02110
Phone: 617-742-9700
Fax: 617-742-9701
Email: dpastor@pastorlawoffice.com

OF COUNSEL

Nicholas A. Migliaccio
Jason S. Rathod
Tyler J. Bean
MIGLIACCIO & RATHOD, LLP
412 H Street, NE, Suite 302
Washington, DC 20002
Phone: 202-470-520
Fax: 202-800-2730
Email: nmigliaccio@classlawdc.com
Email: jrathod@classlawdc.com
Email: tbean@classlawdc.com

Counsel for Plaintiff and the Putative Class