Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Alyssa Brown (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111

Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
AHDOOT & WOLFSON, PC
521 Fifth Avenue, 17th Floor
New York, NY 10175
Tel: (917) 336-0171

Counsel for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

Sean Mortazi, individually and on behalf of all others similarly situated,

Plaintiff,

v.

TikTok Inc., a California corporation,

Defendant.

Case No. 2:26-cv-06371

CLASS ACTION COMPLAINT

ACTION SEEKING STATEWIDE OR NATIONWIDE RELIEF

JURY TRIAL DEMANDED

Plaintiff Sean Mortazi ("Plaintiff") brings this action, individually and on behalf of all others similarly situated, against Defendant TikTok Inc. ("TikTok" or "Defendant"), and seeks monetary damages, restitution, and declaratory and injunctive relief for the proposed Classes, as defined below. Plaintiff makes the following allegations upon information and belief, the investigation of counsel, personal knowledge, and/or facts that are a matter of public record.

I. INTRODUCTION

1. A data breach can have grave consequences for victims both immediately and for years after the actual date of the breach. With the obtained information, thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, collect government benefits, or secure driver's licenses in the victims' names. Data breaches force victims to maintain constant vigilance over the misuse of their information. To lose control over personal information by no fault of your own can be devastating. It is not only an intrusion of privacy and a loss of control, but also a harbinger of future harm: for victims of a data breach, the risk of account takeovers, scam attempts, or attempted account takeovers rises 88%.[1]

2. On June 11, 2026, it was reported that cybercriminals infiltrated one of Defendant's databases and obtained private information of over 2.4 billion TikTok users worldwide (the "Data Breach").[2] The affected database contained the private information of Defendant's users, including names, usernames, email addresses, phone numbers, dates of birth, gender information, language information, and location information ("Private Information").

3. By hacking into the database, cybercriminals accessed and were able to

[1] Identity Theft Resource Center, *Annual Data Breach Report: Record Number of Data Compromises in 2025; 79 Percent Jump Over Five Years* (Jan. 29, 2026), https://www.idtheftcenter.org/post/2025-annual-data-breach-report-record-number-compromises/.

[2] Paulina Okunytė, *2.4 billion TikTok user records leaked online, hackers claim*, Cybernews (June 11, 2026), *available at* https://cybernews.com/security/tiktok-data-leak-claim-infostealers/.

steal the Private Information of billions of TikTok users worldwide. The Data Breach is reported to impact "nearly all TikTok users,"[3] thus impacting the Private Information of many millions of users in California and throughout the United States.

4. The exposed Private Information has significant value on illicit markets, particularly on the Dark Web, since Private Information can be used to commit identity theft, open fraudulent accounts, fraudulently file taxes, apply for and secure loans, obtain government benefits, or facilitate medical and financial fraud.[4] As a direct and foreseeable result of Defendant's conduct, Plaintiff and Class Members face a heightened and continuing risk of identity theft and fraud, have suffered loss of privacy, have spent and will continue to spend time and money on mitigation efforts, and have experienced diminution in the value of their Private Information. Individually and on behalf of the proposed Classes, Plaintiff seeks damages, restitution, and injunctive relief to remedy Defendant's unlawful conduct and prevent future harm.

II. PARTIES

5. Plaintiff Sean Mortazi is a natural person and a citizen of California residing in Los Angeles County. Plaintiff has and uses a TikTok account.

6. Defendant TikTok Inc. is a California corporation and an internet technology and social media company that operates the TikTok application and website in the United States. Defendant's principal place of business is in Culver City, California, and it transacts business in this District and throughout the United States. Defendant's parent company is ByteDance, a Chinese company residing in Singapore.

III. JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of Class Members is more than 100

[3] *Id.*

[4] U.S. Government Accountability Office, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 4, 2007), *available at* https://www.gao.gov/products/gao-07-737.

and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

8. The Court has general jurisdiction over Defendant because its principal place of business is in this District and it is organized under the laws of the State of California. This Court also has specific jurisdiction over Defendant because Defendant has sufficient minimum contacts with California to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice. Defendant is registered to do business and conducts business in California, and it does so on a continuous and systematic basis, and the claims alleged herein arise out of Defendant's polices and practices in California. Plaintiff's claims arise substantially from events, acts, or omissions that took place in California.

9. Venue is proper in the Central District of California under 28 U.S.C. § 1391(b)(2) because Defendant resides in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred within this District.

IV. FACTUAL ALLEGATIONS

A. TikTok Collects, Stores, Uses, and Shares Plaintiff's and Class Members' Private Information as Part of Its Multi-Billion Dollar Business.

10. Defendant is one of the world's largest social media companies. Its popular social media application is one of the most popular in a booming industry, with Defendant's reported profit to be approximately $50 billion in 2025 alone.[5]

11. Defendant's business model and revenue are largely based on advertisements generated by tracking, collecting, and utilizing its users' Private Information and activity on the platform and elsewhere on the Internet that are then

[5] Echo Wong and Min-Jeong Lee, *TikTok Owner ByteDance on Track for $50 Billion Profit in 2025*, Bloomberg (Dec. 19, 2025), *available at* https://www.bloomberg.com/news/articles/2025-12-19/tiktok-owner-bytedance-on-track-for-50-billion-profit-in-2025.

targeted and to users on the TikTok app.[6]

12. Defendant routinely collects, shares, uses, centralizes, and maintains sensitive and confidential Private Information about its customers and potential customers in the process of providing its services.

13. The Private Information collected by Defendant likewise includes or can include information such as names, email addresses, phone numbers, mailing addresses, dates of birth, gender information, language information, location information, and other sensitive identifying data. Defendant requires its users to provide this information in connection with using its services.

14. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that Private Information from unauthorized access and intrusion and to promptly notify users if a breach occurs.

B. TikTok Promises to Protect Plaintiff's and Class Members' Private Information.

15. Defendant had a duty to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized disclosures. Plaintiff and Class Members provided their Personal Information to Defendant with the understanding that Defendant would comply with its Privacy Notices and obligations to keep such information confidential and secure from unauthorized disclosures.

16. When consumers provide confidential information to Defendant, they do so with the reasonable belief that Defendant will take sufficient measures to safeguard their Private Information from foreseeable threats, including cyberattacks.

17. Defendant is and was aware of the sensitive nature of the Private Information it collects, and it acknowledges the importance of data privacy. In the

[6] Sara Karlovitch, *TikTok ad revenue could top $32B – if it doesn't lose its biggest market*, MarketingDive (Mar. 12, 2025), *available at* https://www.marketingdive.com/news/tiktok-ad-revenue-could-top-30-billion-ban-us/742056/.

Privacy Notices on Defendant's website, Defendant represents that: "Your privacy is a top priority at TikTok. Whether we're introducing new features or building on the products you love, we continuously incorporate our privacy principles throughout our product lifecycle."[7]

18. Defendant further states, "We're continually working to ensure strong protections are in place to help keep people safe. We empower our community with a range of tools to control and manage their online presence and we've built privacy features and tools to support age-appropriate experiences on our platform."[8]

19. Defendant's Privacy Policy also touts how Defendant purports to protect sensitive Private Information: "We are committed to protecting and respecting your privacy. . . . We use reasonable measures to help protect information from loss, theft, misuse, unauthorized access, disclosure, alteration, or destruction."[9]

20. The Privacy Policy makes clear that Defendant is and was aware of the need to safeguard the sensitive Private Information entrusted to it by consumers as part of providing its services.

C. The Data Breach.

21. On June 11, 2026, it was reported that 2.4 billion TikTok user records had been leaked online, with a hacker group posting the Data Breach on a forum, with sample records showing sensitive Private Information, including usernames, email addresses, phone numbers, dates of birth, and, in some cases, full names, gender information, and language or location-related information.[10]

22. The threat actors were able to connect to Defendant's database on which Plaintiff's and Class Members' unencrypted Private Information was stored and

[7] TikTok, *Privacy Center*, https://www.tiktok.com/privacy/overview/en.

[8] *Id.*

[9] TikTok, *Privacy Policy*, https://www.tiktok.com/legal/page/us/privacy-policy/en.

[10] Paulina Okunytė, *2.4 billion TikTok user records leaked online, hackers claim*, Cybernews (June 11, 2026), *available at* https://cybernews.com/security/tiktok-data-leak-claim-infostealers/.

download and exfiltrate that information.

23. The attackers gained access to the Private Information of over 2.4 billion users individuals as a result of the breach, including millions American users.

24. Given that the threat actors successfully implemented malware and exfiltrated the Private Information of billions of individuals to third-party networks, Defendant therefore did not have systems in place to detect or prevent the Data Breach.

25. Ransomware groups, like the threat actors here, target Private Information for its value in committing fraud and identity theft. A ransomware attack is a type of cyberattack that is frequently used to target companies for the Private Information that they maintain.[11] Companies should treat ransomware attacks as any other data breach incident because ransomware attacks do far more than simply hold networks hostage — "ransomware groups sell stolen data in cybercriminal forums and Dark Web marketplaces for additional revenue."[12]

26. Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[13] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[14]

---

[11] Danny Palmer, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, ZDNET (July 14, 2020), *available at* https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[12] Center for Internet Security, *Ransomware: The Data Exfiltration and Double Extortion Trends*, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends.

[13] *Id*.

[14] *Id*.

27. Data breaches are preventable.[15] As Lucy Thompson wrote in the Data Breach and Encryption Handbook, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[16] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[17]

28. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[18]

29. Defendant could have prevented or mitigated the consequences of the Data Breach by, among other things, implementing employee and vendor trainin, requiring that employees and vendors verify the identity of third parties by requiring they call back to the verified third-party office line or requesting preset verification codes, implementing strict multi-factor authentication for employees and vendors, limiting access to sensitive data and requiring step-up authentication for access to sensitive data, monitoring their network for logins from unrecognized locations or devices and the transfer of large volumes of data the third-party networks, implementing software to detect and block phishing links, and encrypting data at rest and in transit and deleting data that they were no longer required to maintain. These are all basic and expected industry standard data security measures.

30. Had these training and security steps been taken, Defendant could have prevented the Data Breach. Even if the cybercriminals had managed to access the Private

---

[15] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (2012 ed.), *available at* https://lawcat.berkeley.edu/record/394088.

[16] *Id.* at 17.

[17] *Id.* at 28.

[18] *Id.*

Information, it would have been worthless to them and unable to be exploited and abused had the sensitive data been encrypted. Because these steps were not sufficiently taken by Defendant, Plaintiff and Class Members are now forever unable to control their Private Information.

31. As a consequence of the Data Breach and Defendant's failure to implement sufficient data security safeguards, Plaintiff and Class Members face an imminent and substantial risk of fraud, identity theft, and other harms caused by the unauthorized disclosures of their Private Information—a risk that will persist for the rest of their lives. Plaintiff and Class Members must devote time, money, and energy to protect themselves, to the extent possible, from these harms.

D. The Data Breach Was a Foreseeable Result of TikTok's Data Security Failures.

32. Defendant was well aware that the Private Information it collects, stores, uses, and derives benefits from is highly sensitive and of significant value to those who seek to use it for nefarious purposes.

33. Defendant also knew that a breach of the database containing Plaintiff's and Class Members' Private Information entrusted to Defendant and its resulting exposure would result in the increased risk of identity theft and fraud against the individuals whose Private Information was stolen.

34. These risks are not theoretical; in recent years, numerous high-profile breaches have occurred in the social media sector, including a reported breach against Defendant of nearly one million user passwords in or around April 2025. These breaches put Defendant on notice that its electronic records would be targeted by cybercriminals.

35. In 2025, the Identity Theft Resource Center reported a record 3,322 data compromises, a 5% increase from 2024. These incidents exposed approximately 278.8 million victim notices and represent a 79% increase over five years. The financial services sector remained the most frequently targeted industry, followed by healthcare and professional services. Across industries, breaches increasingly involved the theft of

sensitive personal and financial data, driven largely by phishing, credential theft, and social engineering attacks.[19]

36. In 2024, security researchers noted that, "when including the extortion-only, no-encryption data theft attacks, which are often conducted by ransomware actors, the number [of ransomware attacks] is up year-over-year. Ransomware and data extortion attacks were present in 32% of reported attacks, and 92% of industries experienced ransomware as a top threat targeting them."[20]

37. Consequently, Defendant should have known of the importance of safeguarding Plaintiff's and Class Members' Private Information and of the foreseeable consequences that would occur if its data security system was breached, including the significant costs that would be imposed on victims as a result of a breach.

E. TikTok Knew It Was at High Risk for a Data Breach.

38. Beyond these statistics regarding the increasingly high incident rate of data breaches, Defendant knew that it was at high risk for being targeted by cybercriminals.

39. Defendant knew or should have known its internal network would permit transmission of high volumes of valuable and highly sensitive Private Information of the billions of individuals that use TikTok worldwide. As a result, Defendant knew its systems would be attractive targets for cybercriminals.

40. Defendant also knew that a breach of its systems, and exposure of the information therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised.

41. Defendant knew or should have known that immediate action was

---

[19] Identity Theft Resource Center, *2025 Annual Data Breach Report: Record Number of Data Compromises* (Jan. 29, 2026), *available at* https://www.idtheftcenter.org/post/2025-annual-data-breach-report-record-number-compromises/.

[20] Alexander Culafi, *Verizon DBIR: Vulnerability exploitation in breaches up 180%*, TechTarget (May 1, 2024), *available at* https://www.techtarget.com/searchsecurity/news/366582952/Verizon-DBIR-Vulnerability-exploitation-in-breaches-up-180.

necessary to mitigate the access and disclosure of the Private Information entrusted to them. However, Defendant failed to do so and caused Plaintiff's and Class Members' highly sensitive Private Information to be exposed to the public.

F. TikTok Failed to Implement Sufficient Security Measures to Prevent a Data Breach.

42. On information and belief, Defendant failed to utilize sufficient security measures, including the well-known "Principle of Least Privilege," which limits users access to and permissions in sensitive systems, and monitoring for activities like large data downloads, proper endpoint and network monitoring and scanning, and automatically issues alerts upon large data download attempts or blocks such activity. As experts have opined, such real-time monitoring is essential to cybersecurity. "Cybersecurity or process monitoring is continuously observing and analyzing your computer network or systems to prevent cyberattacks. The primary objective of monitoring in cybersecurity is to quickly identify signs of vulnerability and responding to potential security threats in real-time."[21] Here, Defendant's own security and monitoring tools insufficient to identify and stop the Data Breach.

43. The attackers exfiltrated a massive amount of Private Information. Such actions should have only been possible by Defendant's network administrators and should have required even those administrators to pass through additional security features. Such exfiltration activity should have been detected and prevented and should have raised numerous red flags to Defendant had they properly monitored its systems.

44. Had Defendant implemented adequate cybersecurity monitoring, the exfiltration of Plaintiff's and Class Members' Private Information would have been prevented or would have been much smaller in scope.

[21] SentinelOne, *Cyber Security Monitoring: Definition and Best Practices* (Sept. 7, 2025), *available at* https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/.

G. The Private Information Is or Will Be Published on the Dark Web.

45. It is almost a certainty that Plaintiff's and Class Members' Private Information has or will be released on, or will be listed for sale on, the "Dark Web."

46. The Dark Web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term "Dark Web" is used to distinguish from the "clear web," the part of the World Wide Web that is readily accessible through traditional internet browsers. The Dark Web is accessed through The Onion Router ("Tor"), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers ("relay(s)"), encrypting data at each step to ensure that both the user's location and browsing activity are difficult to trace. Tor uses a technique called "onion routing," where data is encrypted in layers like an onion. Each relay in the network peels away a layer of encryption before passing the data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

47. The Dark Web poses significant challenges to cyber security professionals and law enforcement agencies. The Dark Web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, Dark Web sites do not advertise their existence. The anonymity of the Dark Web led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Private Information.[22]

48. Once stolen private information is posted on the Dark Web, it will most likely be distributed to multiple different groups and individuals,[23] each of which can

[22] *Crime and the Deep Web*, Stevenson University, *available at* https://www.stevenson.edu/online/about-us/news/crime-deep-web/; *Defending Against Malicious Cyber Activity Originating from Tor*, CISA (Aug. 2, 2021), *available at* https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a.

[23] *The Dark Web and Cybercrime*, U.S. Dep't of Health and Human Servs. Cybersecurity Program, Office of Information Security, at 10 (July 23, 2020), *available at* https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf.

use that information for fraud and identity theft.

49. This data lifecycle is confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it with their code that silently tracked any access to the file. The data was quickly spread across five continents: North America, Asia, Europe, Africa and South America. In the end, 47 different parties downloaded the data. It was mainly downloaded by users in Nigeria, Russia and Brazil, with the most activity coming from Nigeria and Russia.[24] This experiment demonstrated that data released on the Dark Web will quickly spread around the world. Since cybercriminals typically conduct data breaches to sell the victims' breached sensitive information on the Dark Web, this will likely be the fate of Plaintiffs' and Class Members' sensitive Private Information.[25]

H. The Data Breach Significantly Harms Victims.

50. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[26] $168.6

---

[24] Kelly Jackson Higgins, *What Happens When Private Information Hits the Dark Web*, Dark Reading (Apr. 7, 2015), *available at* https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web; *see also* Kristin Finklea, *Dark Web*, Congressional Research Service, at 10 (July 7, 2015), *available at* https://nsarchive.gwu.edu/sites/default/files/documents/2696100/Document-8.pdf; Pierluigi Paganini, *How Far Do Stolen Data Get in the Deep Web After a Breach?*, Security Affairs (Apr. 12, 2015), *available at* https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html.

[25] F-Secure, *Why hackers want your personal information – and how to protect it* (Nov. 21, 2024), *available at* https://www.f-secure.com/en/articles/why-do-hackers-want-your-personal-information.

[26] *Alphabet Inc. Annual Report (Form 10-K)*, SEC, at 29, 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

billion of this revenue derived from its Google business,[27] which is driven almost exclusively by leveraging the Private Information it collects about users of its various "free" products and services.

51. Criminal law also recognizes the value of Private Information and the serious nature of the theft of Private Information by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Private Information. Once a cybercriminal unlawfully acquires Private Information, the criminal can demand a ransom or blackmail payment for its destruction, use the Private Information to commit fraud or identity theft or sell the Private Information to other cybercriminals on the black market.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2(a). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, names and dates of birth. 16 C.F.R. § 603.2(b).

53. Identity thieves use Private Information for a variety of crimes. According to Experian, with access to an individual's private information, criminals can do more than just empty a victim's bank account. They can also commit all other manner of fraud, including using the victim's Private Information to obtain government benefits, file a fraudulent tax return to obtain a large refund, get medications or medical procedures, or to transfer home titles and then take mortgages against the victim's home. In addition, identity thieves may take over a victim's social media accounts and blackmail the person by threatening to share personal or embarrassing information or pictures with the victim's contacts.[28]

---

[27] *Id.* at 33.

[28] Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (Apr. 8, 2025), *available at*

54. Identity theft presents many challenges. In a survey, the Identity Theft Resource Center ("ITRC") found that 76% of victims of identity crimes who reached out to the ITRC for assistance needed more than a month to resolve issues stemming from identity theft, and 48% of those victims still had not resolved their issues after a year.[29]

55. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

56. Beyond monetary losses and identity fraud, data breaches also have a deep, psychological impact on their victims:

> In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you and prolong or worsen a cyber attack. [30]

I. Victims of Data Breaches Must Expend Time and Money to Mitigate Their Risk of Harm.

57. Cybercriminals can and do use the precise Private Information that Defendant was entrusted to safeguard to perpetrate financial crimes that harm Plaintiff and Class Members.

58. The FTC recommends that identity theft victims take several steps to

---

https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[29] *Consumer Impact – Business Impact Report*, ITRC, at 26 (Oct. 2024), *available at* https://www.idtheftcenter.org/publication/itrc-2024-consumer-and-business-impact-report/.

[30] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), *available at* https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks.

protect their Private Information after a data breach, including contacting one of the three credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit and correcting their credit reports.[31]

59. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the GAO report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[32]

60. There may be a time lag between when sensitive Private Information is stolen, when it is used and when the victim discovers its use. On average, it takes approximately three months for a victim to discover their identity was stolen and used and it takes some victims up to three years to learn that information.[33]

61. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (e.g., names, addresses, and dates of birth), directly and materially increase the chance that a potential victim is targeted in the future by a spear phishing attack, which often result in a high rate of identity theft, fraud and extortion.[34]

---

[31] FTC, *Identity Theft Recovery Steps*, https://www.identitytheft.gov/Steps.

[32] *Private Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, at 29 (June 2007), *available at* https://www.gao.gov/assets/270/262899.pdf.

[33] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS, Vol. 17, No. 5, at 12 (2019) http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[34] *See, e.g.,* Jessica Davis, *Blackbaud Confirms Hackers Stole Some SSNs, as Lawsuits Increase,* TechTarget and Informa Tech's Digital Businesses Combine (Sept. 30,

62. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[35] With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

63. The development of "Fullz" packages means here that the stolen Private

---

2020), https://www.techtarget.com/healthtechsecurity/news/366595050/Blackbaud-Confirms-Hackers-Stole-Some-SSNs-as-Lawsuits-Increase (concluding that Private Information "in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware"); *see also* Mich. Dep't of Attorney General, *Attorney General Nessel Reminds Consumers to Watch For Phishing Scams Following Blackbaud Security Breach* (Sept. 18, 2020), *available at* https://www.michigan.gov/ag/news/press-releases/2020/09/18/attorney-general-nessel-reminds-consumers-to-watch-for-phishing-scams (noting the accessed Private Information "generally included names, titles, telephone numbers, email addresses, mailing addresses, dates of birth and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests and other donor profile information.").

[35] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the Dark Web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), *available at* https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

Information from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

64. Thus, even if certain information was purportedly not involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

65. Plaintiff's and Class Members' stolen Private Information will continue to be leaked and traded on the Dark Web, meaning Plaintiff and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Indeed, some Class Members are in the very early stages of their lives, as minor children or young adults who may not even have established credit or use services to monitor identity theft and credit fraud. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

J. The Data Breach Caused Plaintiff and the Class Demonstrable Harm.

66. The Private Information exposed in the Data Breach has real value, as explained herein. Plaintiff and Class Members are therefore deprived of their rights to control that property and have lost value they might otherwise incur from that Private Information.[36]

---

[36] Ravi Sen, *Here's How Much Your Private Information Is Worth to Cybercriminals – and What They Do with It,* PBS NEWS (May 14, 2021) https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it.

[36] *Id*.

67. Plaintiff and Class Members already spent significant time monitoring their accounts, changing login credentials and recovering from the inevitable fraud and identity theft which will occur, and deserve to be compensated.[37]

68. Plaintiff and Class Members should be compensated for the aggravation, agitation, anxiety and emotional distress that they suffered, and will continue to suffer, as a result of the Data Breach. The knowledge that their information is out in the open, available for sale and exploitation at any time in the future, is real harm that also deserves compensation.

69. Plaintiff and Class Members were also deprived of the benefit of their bargain when they interacted with Defendant. Defendant had a duty to take reasonable steps to protect the Private Information of the individuals whose information was entrusted to it, and those individuals entrusted that information to Defendant in exchange for Defendant taking on that duty and utilizing Plaintiff's and Class Members' Private Information for its business profit. This duty was inherent in the relationships between Plaintiff and Class Members and Defendant, whether through express contractual terms, implied contractual terms, bailment or statutory or implied duties of good faith and fair dealing.

70. Defendant failed in its duty to protect Plaintiff's and Class Members' Private Information and their ability to protect that information in the future.

K. TikTok Failed to Follow Industry Standards for Data Security.

71. Defendant had obligations arising under the FTC Act, industry standards, common law, and their own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and protected from unauthorized access and disclosure.

72. Despite Defendant's knowledge of the continued risks to Plaintiff's and

[37] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See, e.g.*, Equifax Data Breach Settlement, https://www.equifaxbreachsettlement.com/.

Class Members' Private Information, Defendant failed to use reasonable security procedures and practices appropriate to the nature of the Private Information maintained on Plaintiff and Class Members. As described below, had Defendant implemented industry-standard security measures and adequately invested in data security, unauthorized parties likely would not have been able to access Defendant's systems, and the Data Breach would have been prevented or much smaller in scope.

1. TikTok Failed to Comply with FTC Guidelines.

73. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[38]

74. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive Private Information is an "unfair practice" in violation of the Federal Trade Commission Act ("FTC Act" or "FTCA"), 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.,* 799 F.3d 236, 248 (3d Cir. 2015).

75. In 2016, the FTC updated its publication titled *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines recommend that:

i. Businesses should promptly dispose of personal identifiable information that is no longer needed, and retain sensitive data "only as long as you have a business reason to have it;"

ii. Businesses should encrypt sensitive Private Information stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;

iii. Businesses should thoroughly understand the types of vulnerabilities on

[38] *Start with Security: A Guide for Business,* FTC (Aug. 2023), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

their network and how to address those vulnerabilities;

iv. Businesses should install intrusion detection systems to promptly expose security breaches when they occur; and

v. Businesses should install monitoring mechanisms to watch for large troves of data being transmitted from their systems.[39]

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

77. The FTC treats the failure to employ reasonable data security safeguards as an unfair act or practice prohibited by Section 5 of the FTC Act.

78. Indeed, 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. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

79. As evidenced by the Data Breach, Defendant failed to properly implement one or more of the basic data security practices recommended by the FTC. Defendant's failure to employ reasonable and appropriate data security measures to protect against unauthorized access to individuals' Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

2. TikTok Failed to Comply with Industry Standards.

80. As noted above, experts studying cybersecurity routinely identify entities

[39] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016) https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business-0

in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

81. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[40]

82. NIST provides a comprehensive cybersecurity framework that companies of any size can use to evaluate and improve their information security controls.[41]

83. NIST publications include substantive recommendations and procedural guidance pertaining to a broad set of cybersecurity topics including risk assessments, risk management strategies, access controls, training, data security controls, network monitoring, breach detection, and incident response.[42]

84. NIST recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.

b. Use security software to protect data.

---

[40] Center for Internet Security, *The 18 CIS Critical Security Controls*, https://www.cisecurity.org/controls/ciscontrols.

[41] *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS & TECHNOLOGY (Apr. 16, 2018) App'x A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.

[42] *Id*. at Table 2, 26-43.

c. Encrypt sensitive data, at rest and in transit.

d. Conduct regular backups of data.

e. Update security software regularly, automating those updates if possible.

f. Have formal policies for safely disposing of electronic files and old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity.

85. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[43]

86. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, or to require the same from their vendor, including failing to meet or require the minimum standards of the NIST Cybersecurity Framework

[43] *Shields Up: Guidance for Organizations*, CISA, https://www.cisa.gov/shields-guidance-organizations.

Version 2.0 and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiff's and Class Members' Private Information, resulting in the Data Breach.

87. These foregoing frameworks are existing and applicable industry standards for a business's obligations to provide adequate data security for its customers' sensitive information. Defendant failed to comply with at least one, or all, of these accepted standards, thereby opening the door to cybercriminals to carry out the Data Breach.

88. Finally, several best practices have been identified that a minimum should be implemented by businesses in possession of Private Information, like Defendant, including but not limited to educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multifactor authentication; backup data and limiting which employees can access sensitive data. Upon information and belief, Defendant failed to follow these industry best practices, including a failure to implement encryption, strong passwords, and multi-factor authentication.

3. TikTok Breached Its Duty to Safeguard Plaintiff's and Class Members' Private Information.

89. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons, especially notorious cybercriminals.

90. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including data security consistent with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected Plaintiff's and Class Members' Private Information.

91. Defendant owed a duty to Plaintiff and Class Members to create and

implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and vendors who accessed Private Information within its computer systems on how to adequately protect Private Information.

92. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

93. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

94. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

95. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

96. Defendant breached its obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, servers, and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain adequate data security systems that would reduce the risk of data breaches and cyberattacks;
b. Failing to adequately protect their customers' Private Information;
c. Failing to properly monitor their data security systems for existing intrusions;
d. Failing to sufficiently train their employees regarding the proper handling of their clients' Private Information;
e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA; and
f. Otherwise breaching their duties and obligations to protect Plaintiff's and Class Members' Private Information.

97. Defendant negligently and unlawfully failed to safeguard Plaintiff's and

Class Members' Private Information by allowing cybercriminals to access their computer networks and systems, which contained unsecured and unencrypted Private Information.

98. Had Defendant remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into their information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

L. Plaintiff and Class Members Suffered Injury.

99. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: (1) closely monitor their bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

100. Once Private Information is exposed, there is virtually no way to recover the data or prevent future misuse. This is especially true here, where the information stolen during the Data Breach has been leaked on the Dark Web and remains available to download. As a result, Plaintiff and Class Members must maintain heightened vigilance indefinitely. Further, Plaintiff and Class Members have not been compensated for the unconsented and unauthorized disclosure of their Private Information, for which there is a robust market.

101. As a direct result of the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer economic and other concrete harms, including but not limited to:

a. Unauthorized disclosure of their confidential information;
b. Loss of the control of their Private Information;
c. Loss of the benefit of their bargain in choosing organizations promising data protection;
d. Identity theft, fraud, and misuse of financial information;
e. Out-of-pocket expenses for credit monitoring, mitigation efforts, and fraud prevention tools;
f. Unauthorized charges and restricted access to financial accounts;
g. Emotional distress, anxiety, and loss of privacy;
h. Time and productivity lost dealing with the consequences of the breach;
i. Damage to credit scores, including from fraudulent inquiries; and
j. Continued and imminent risk of future fraud and identity theft due to their data being in the hands of unauthorized third parties.

102. Individuals suffer harm each time their personal data is compromised and circulated on underground markets—even if they have been affected by prior breaches. The Dark Web contains vast, fragmented repositories of stolen information that can be aggregated by different criminals for varied forms of fraud. Each subsequent breach increases the likelihood that a victim's sensitive data will be accessed by more actors and exploited in new and damaging ways.

103. Even in instances where an individual is reimbursed for a financial loss due to identity theft or fraud, that does not make that individual whole again as there is typically significant time and effort associated with seeking reimbursement. There may also be a significant time lag between when Private Information is stolen and when it is misused for fraudulent purposes.

104. Plaintiff and Class Members place significant value on data security and consider a company's ability to protect Private Information a key factor in their decisions on which companies to use. Conversely, consumers are far less likely to share personal

data with companies that have suffered a data breach—reflecting the reputational damage and business consequences that flow from failing to safeguard sensitive information.

105. Because of the premium consumers place on data privacy, companies with robust security practices are viewed more favorably and can command higher memberships than those that do not. Had Defendant's customers, including Plaintiff, known the truth about Defendant's lack of cybersecurity—or that Defendant entrusted its sensitive data to an entity with inadequate security practices—they would not have opened an account or used Defendant's services or otherwise sought alternative services. As a result, Plaintiff and Class Members were deprived of the benefit of their bargain, having provided their Private Information for secure and responsible handling but receiving substantially less in return.

106. By collecting and storing Plaintiff's and Class Members' sensitive information, Defendant undertook a duty to safeguard it and avoid increasing the risk of identity theft or fraud. Because Defendant failed to uphold that duty, Plaintiff seeks the present value of identity protection services and other compensatory measures to address the current and future harm stemming from the Data Breach.

107. Additionally, Plaintiff and Class Members are entitled to recover the reasonable use value of their Private Information that was accessed and exfiltrated without authorization. This form of compensation mirrors damages awarded in intellectual property cases for unauthorized use of intangible assets. As with a patent or trade secret, Private Information is non-rivalrous: their unauthorized use by a third-party does not eliminate the owner's ability to use them but still justifies compensation based on market value.

108. Upon information and belief, Defendant continues to retain the Private Information of Plaintiff and Class Members. As long as Defendant maintain possession of this information, Plaintiff and Class Members have a strong and ongoing interest in ensuring that adequate safeguards are in place to prevent further unauthorized access or

disclosure.

V. CLASS ACTION ALLEGATIONS

109. Plaintiff brings this action individually and on behalf of all other persons similarly situated, pursuant to Rule 23 of the Federal Rules of Civil Procedure.

110. The Classes that Plaintiff seeks to represent are defined as follows:

The Nationwide Class

All individuals residing in the United States whose Private Information was compromised in the TikTok Data Breach reported on or about June 11, 2026.

The California Subclass

All individuals residing in the State of California whose Private Information was compromised in the TikTok Data Breach reported on or about June 11, 2026.

111. The above Classes are herein referred to collectively as the "Class." Excluded from the Class are: (1) any Judge presiding over this action, members of their immediate families, and Court Staff; and (2) Defendant, its subsidiaries, parent companies, successors, predecessors, and any entity in which Defendant, or its parents, have a controlling interest, and its current or former officers and directors.

112. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include millions of members who are geographically dispersed.

113. **Typicality**: Plaintiff's claims are typical of Class members' claims. Plaintiff and all Class members were injured through Defendant's uniform misconduct, and Plaintiff's claims are identical to the claims of the Class members they seek to represent. Accordingly, Plaintiff's claims are typical of Class members' claims.

114. **Adequacy**: Plaintiff's interests are aligned with the Class whom Plaintiff seeks to represent, and Plaintiff has retained counsel with significant experience

prosecuting complex class action cases, including cases involving alleged privacy and data security violations. Plaintiff and undersigned counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiff and undersigned counsel.

115. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiff; and other Class members' claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class members individually to effectively redress Defendant's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

116. **Commonality and Predominance:** The following questions common to all Class members predominate over any potential questions affecting individual Class members:

- whether Defendant engaged in the wrongful conduct alleged herein;
- whether Defendant's data security practices resulted in the disclosure of Plaintiff's and other Class members' Personal Information and the Data Breach;
- whether Defendant violated privacy rights and invaded Plaintiff's and Class members' privacy;
- whether Defendant violated the consumer protection statutes as alleged herein; and
- whether Plaintiff and Class members are entitled to damages, equitable

relief, or other relief and, if so, in what amount.

117. Given that Defendant engaged in a common course of conduct as to Plaintiff and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

118. **Injunctive and Declaratory Relief:** Consistent with Fed. R. Civ. P. 23(b)(2), Defendant, through its conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the class as a whole.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE

119. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

120. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

121. Defendant was entrusted with, stored, and otherwise had access to the Private Information of Plaintiff and Class Members.

122. Defendant knew, or should have known, of the risks inherent to storing the Private Information of Plaintiff and Class Members, and to not ensuring that its servers and systems, and the Private Information, were secure. These risks were reasonably foreseeable to Defendant.

123. Defendant owed duties of care to Plaintiff and Class Members whose Private Information had been entrusted to Defendant.

124. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate data security. Defendant had a duty to safeguard Plaintiff's and Class Members' Private Information and to ensure that it adequately protected Private Information. Defendant breached this duty.

125. Defendant's duty of care arises from its knowledge that its customers entrust it with highly sensitive Private Information that Defendant is required to, and represents that it will, handle securely. Indeed, on its website, Defendant commits to data privacy in its Privacy Policy and other privacy-related statements and advertisements, which include safeguarding sensitive Private Information.

126. Only Defendant was in a position to ensure that its systems, servers, and services were sufficient to protect against breaches and the harms that Plaintiff and Class Members have now suffered.

127. A "special relationship" exists between Defendant, on the one hand, and Plaintiff and Class Members, on the other hand. Defendant entered into a "special relationship" with Plaintiff and Class Members by agree to accept, store, and have access to sensitive Private Information provided by Plaintiffs and Class Members in connections with the use of Defendant's services and the substantial revenue and profit that it reaps from utilizing that Private Information.

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

129. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Private Information.

130. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known it was failing to meet these duties, and that Defendant's breach would cause Plaintiff and Class Members to experience foreseeable harms associated with the exposure of their Private Information.

131. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have been harmed and face an imminent and ongoing risk of harm.

132. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in the amount to be proven at trial.

COUNT II
NEGLIGENCE PER SE

133. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

134. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

135. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide adequate data security practices in connection with safeguarding Plaintiff's and Class Members' Private Information.

136. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act (15 U.S.C. §45) and the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 *et seq.*), among other statutes, by failing to provide fair, reasonable, or adequate data security in connection with the provision of services in order to safeguard Plaintiff's and Class Members' Private Information.

137. Defendant's failure to comply with applicable laws and regulations constitutes negligence per se.

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

139. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known that it was failing to meet its duties, and that a breach would cause Plaintiff and Class Members to experience the foreseeable harm associated with the exposure of their Private Information.

140. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have been harmed and face imminent and ongoing risk of harm.

141. As a direct and proximate result of Defendant's negligence per se, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT

142. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

143. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

144. Defendant provided or provide services to Plaintiff and Class Members, or Plaintiff and Class Members provided their Private Information to Defendant in some other capacity.

145. In connection with their business relationship, Plaintiff and Class Members entered into implied contracts with Defendant.

146. Pursuant to these implied contracts, Plaintiff and Class Members provided Defendant with their Private Information. In exchange, Defendant agreed, among other things: (1) to take reasonable measure to protect the security and confidentiality of Plaintiff's and Class Members' Private Information; and (2) to protect Plaintiff's and Class Members' Private Information in compliance with federal and state laws and regulations and industry standards.

147. The protection of Private Information was a material terms of the implied contracts between Plaintiff and Class Members, on the one hand, and Defendant, on the other hand. Had Plaintiff and Class Members known that Defendant would not adequately protect users' Private Information, they would not have used Defendant's services.

148. Plaintiff and Class Members performed their obligations under the implied contract when they provided Defendant with their Private Information.

149. Necessarily implicit in the agreements between Plaintiff/Class Members and Defendant was Defendant's obligation to take reasonable steps to secure and safeguard Plaintiff's and Class Members' Private Information.

150. Defendant breached its obligations under its implied contracts with Plaintiff

and Class Members by failing to implement and maintain reasonable security measures to protect their Private Information.

151. Defendant's breach of its obligations of its implied contracts with Plaintiff and Class Members directly resulted in the Data Breach.

152. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of their implied agreements.

153. Plaintiff and other Class Members were damaged by Defendant's breach of implied contracts because: (i) they have suffered actual harm or identity theft; (ii) they face substantially increased risk of Identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their Private Information was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their Private Information has been breached; (v) they were deprived of the value of their Private Information, for which there is a well-established national and international market; (vi) they were deprived of the benefit of their bargain; and or (vii) they lost time and money incurred to mitigate and remediate the effects of the breach, including the increased risks of identity theft they face and will continue to face.

COUNT IV
INVASION OF PRIVACY

154. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

155. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

156. Plaintiff and Class Members have a reasonable expectation of privacy in the Private Information that Defendant disclosed without authorization.

157. By failing to keep Plaintiff's and Class Members' Private Information safe, knowingly employing inadequate data privacy policies and protocols, and disclosing Private Information to unauthorized parties for unauthorized use, Defendant unlawfully

invaded Plaintiff's and Class Members' privacy by, *inter alia*:

a. Intruding into Plaintiff's and Class Members' private affairs in a manner that would be highly offensive to a reasonable person;

b. Invading Plaintiff's and Class Members' privacy by improperly using their Private Information properly obtained for a specific purpose for another purpose or disclosing it to some third-party;

c. Failing to adequately secure Private Information from disclosure to unauthorized persons; and

d. Enabling the disclosure of Plaintiff's and Class Members' Private Information without consent.

158. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiff's and Class Members' position would consider their actions highly offensive.

159. Defendant knew that their IT systems and servers were vulnerable to data breaches prior to the Data Breach.

160. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private affairs by disclosing their Private Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

161. As a proximate result of such unauthorized disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their Private Information were unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class Members' protected privacy interests.

162. In failing to protect Plaintiff's and Class Members' Private Information, and in disclosing Plaintiff's and Class Members' Private Information, Defendant acted with malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

163. Plaintiff seeks injunctive relief on behalf of the Class, restitution, and all

other damages available under this Count.

COUNT V
UNJUST ENRICHMENT

164. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

165. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

166. This claim is pleaded in the alternative to the implied contract claim.

167. Defendant has profited and benefited from the monies or fees paid and Private Information provided by Plaintiff and Class Members to receive services from Defendant.

168. Defendant has voluntarily accepted and retained these profits and benefits with full knowledge and awareness that, as a result of the misconduct and omissions described herein, Plaintiff and Class Members did not receive services of the quality, nature, fitness, or value represented by Defendant and that reasonable consumers expected.

169. Defendant has been unjustly enriched by retaining and withholding these benefits at the expense of Plaintiff and Class Members.

170. Equity and justice are against permitting Defendant to retain these profits and benefits.

171. Plaintiff and Class Members suffered injury as a direct and proximate result of Defendant's unjust enrichment and seek an order directing Defendant to disgorge these benefits and pay restitution to Plaintiff and Class Members.

COUNT VI
DECLARATORY RELIEF

172. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

173. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

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

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

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

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

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

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

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

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

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

179. And if another breach occurs, Plaintiff and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full

and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiff's and Class Members' injuries.

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

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

COUNT VII
VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200 *et seq.*

182. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

183. Plaintiff brings this cause of action individually and on behalf of the Nationwide Class, or, in the alternative, on behalf of the California Subclass.

184. Defendant's conduct constitutes unfair, illegal, and fraudulent business practices within the meaning of the California Business & Professions Code §§ 17200 *et seq.* (the "UCL").

185. Defendant's conduct violated certain laws as alleged herein, including the Federal Trade Commission Act (15 U.S.C. § 45) and the Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801 *et seq.*). By engaging in the said conduct in the course of doing business within California, Defendant engaged in unlawful business practices in violation of the UCL as to Plaintiff and all Class Members.

186. By engaging in the above-described conduct in the course of doing business, Defendant engaged in unfair business practices in violation of the UCL because the harm to Plaintiff and Class Members outweighed any utility that Defendant's conduct may have produced.

187. Defendant's failure to disclose information concerning the Data Breach directly and promptly to affected customers constitutes a fraudulent act or practice in violation of the UCL. Defendant's failure to adequately protect Plaintiff's and Class Members' Private Information, despite assurances it would do so and that Defendant met industry standards for data security, also constitutes a fraudulent act or practice in violation of the UCL.

188. Plaintiff and Class Members suffered injury in fact as a result of Defendant's conduct.

189. Individually and on behalf of the Class, Plaintiff seeks injunctive relief, restitution, and all other damages available under this cause of action.

COUNT VIII
VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 *et seq.*

190. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

191. Plaintiff brings this cause of action individually and on behalf of the California Subclass.

192. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiff and the Class. As a direct and proximate result, Plaintiff's and the Class's Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

193. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the

preceding calendar year." Civil Code § 1798.140(d).

194. Plaintiff and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguard Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiff's and Class Members' Private Information. Plaintiff and Class Members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

195. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. No notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages. *See* Civil Code § 1798.150(b). Accordingly, Plaintiff and Class Members seek actual pecuniary damages suffered as a result of Defendant's violations described herein, as well as injunctive relief as requested herein. Plaintiff intends to amend this complaint to seek statutory damages upon expiration of the cure period pursuant to Civil Code § 1798(a)(1)(A)(B), (a)(2), and (b).

COUNT IX
VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80 *et seq.*

196. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

197. Plaintiff brings this cause of action individually and on behalf of the California Subclass.

198. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of

California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." *Id.* (emphasis added).

199. The Data Breach constitutes a "breach of the security system" of Defendant.

200. An unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class.

201. Defendant knew that an unauthorized person acquired the personal, unencrypted information of Plaintiff and the Class but has yet to notify them. Given the severity of the Data Breach, this is an unreasonable delay.

202. Defendant's unreasonable delay is preventing Plaintiff and the Class from taking appropriate measures to protect themselves against harm.

203. Because Plaintiff and the Class have been unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

204. Plaintiff and the Class are entitled to equitable relief and damages in an amount to be determined at trial.

COUNT X
INVASION OF PRIVACY, CALIFORNIA CONSTITUTION, ART. 1 § 1

205. Plaintiff repleads and incorporates by reference Paragraphs 1-118 as if set forth herein.

206. Plaintiff brings this cause of action individually and on behalf of the California Subclass.

207. California established the right to privacy in Article I, Section 1 of the California Constitution.

208. Plaintiff and Class Members had a legitimate expectation of privacy to their Private Information and were entitled to the protection of this information against disclosure to unauthorized third parties.

209. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep their Private Information contained as a part thereof, confidential.

210. Defendant failed to protect and released Plaintiff's and Class Members' Private Information to unknown and unauthorized third parties.

211. Defendant allowed unauthorized and unknown third-parties access to and examination of Plaintiff's and Class Members' Private Information, by way of Defendant's failure to protect the Private Information.

212. The unauthorized release to, custody of, and examination by unauthorized third parties of Plaintiff's and Class Members' Private Information is highly offensive to a reasonable person.

213. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their Private Information to Defendant as part of seeking services from Defendant, but privately with an intention that the Private Information would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

215. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

216. Because Defendant acted with a knowing state of mind, it had notice that

its inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

217. As a proximate result of the above acts and omissions of Defendant, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

218. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, respectfully requests relief as follows:

A. An order certifying this action as a class action, and certifying the Classes defined herein, designating Plaintiff as the representative of the respective Classes defined herein;

B. An order declaring that Defendant's actions, as described above constitute negligence and violations of the state data security and privacy statutes set forth above, and that Defendant was unjustly enriched as a result of its actions;

C. A judgment awarding Plaintiff and Class Members appropriate relief, including actual, compensatory, and/or statutory damages, and punitive damages (as permitted by law), in an amount to be determined at trial;

D. A judgment awarding any and all equitable, injunctive, and declaratory relief as may be appropriate, including orders of

disgorgement of Defendant's unlawful gains, and restitution;

E. A judgment awarding injunctive relief as set forth above, non-restitutionary disgorgement of profits and unlawful gains, and such other equitable relief as the Court may deem proper;

F. A judgment awarding all costs, including experts' fees, attorneys' fees, and the costs of prosecuting this action, and other relief as permitted by law;

G. Pre-judgment and post-judgment interest, as permitted by law; and

H. Grant such other legal and equitable relief as the Court may deem appropriate.

VIII. DEMAND FOR JURY TRIAL

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

Dated: June 11, 2026

Respectfully submitted,

By: */s/ Tina Wolfson*

Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Alyssa Brown (SBN 301313)
abrown@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111

Bradley K. King (SBN 274399)
bking@ahdootwolfson.com
AHDOOT & WOLFSON, PC
521 Fifth Avenue, 17th Floor
New York, NY 10175
Tel: (917) 336-0171

Counsel for Plaintiff and the Proposed Class