

Byron T. Ball
(State Bar No. 150195)
THE BALL LAW FIRM APC
100 Wilshire Blvd., Suite 700
Santa Monica, CA 90401
Telephone: (310) 980-8039
Facsimile: (415) 477-6710
Email: btb@balllawllp.com

Attorneys for Plaintiff and Proposed Class

**IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
EASTERN DIVISION**

KYLE MCDANIEL, and all similarly
situated individuals,

Plaintiff,

v.

TOSHIBA AMERICA BUSINESS
SOLUTIONS, INC.,
Defendant.

Case No.: _____

CLASS ACTION COMPLAINT

- 1. Negligence**
- 2. Negligence *Per Se***
- 3. Breach of Implied Contract**
- 4. Unjust Enrichment**
- 5. Declaratory Judgment**

JURY TRIAL DEMANDED

Plaintiff Kyle McDaniel (“Plaintiff”), individually and on behalf of all other
similarly situated individuals (the “Class” or “Class Members,” as defined below),
by and through his undersigned counsel, files this Class Action Complaint against
Toshiba America Business Solutions, Inc. (“Toshiba” or “Defendant”) and alleges

1 the following based on personal knowledge of facts, upon information and belief,
2 and based on the investigation of his counsel as to all other matters.

3 **I. INTRODUCTION**

4 1. Plaintiff brings this class action lawsuit against Toshiba for its
5 negligence and failure to protect and safeguard Plaintiff's and the Class's highly
6 sensitive personally identifiable information ("PII").¹ As a result of Toshiba's
7 insufficient data security, cybercriminals easily infiltrated Defendant's inadequately
8 protected computer systems and accessed the PII of Plaintiff and the Class (the "Data
9 Breach" or "Breach").² Now, Plaintiff's and the Class's PII is in the hands of
10 cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest
11 of their lives.

12 2. On an undisclosed date, Toshiba discovered suspicious activity within
13 its email environment.³

14 3. After an investigation, Toshiba determined an unauthorized actor had
15 access to its email environment from December 4, 2023, through March 18, 2024—
16 **over three (3) months.**⁴

17 4. Toshiba claims the investigation of the Data Breach is still ongoing, but
18 after a preliminary review Toshiba has already determined certain email(s) and
19 attachment(s) were potentially viewed by an unauthorized individual.⁵

20 5. The PII accessed and/or acquired in the Data Breach included highly
21 sensitive private information such as, names and Social Security numbers,
22

23 _____
24 ¹ [https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-
a1252b4f8318/401acca4-7cb4-4d16-899b-82b4fabe9bf6.shtml](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/401acca4-7cb4-4d16-899b-82b4fabe9bf6.shtml).

25 ² *Id.*

26 ³ *Id.*

27 ⁴ *Id.*

⁵ *Id.*

1 (collectively, “Private Information”).⁶

2 6. Defendant acquired, collected, and stored Plaintiff’s and Class
3 Members’ Private Information for employment purposes and through customer
4 relationships. Therefore, at all relevant times, Defendant knew or should have known
5 that Plaintiff’s and Class Member’s sensitive data, including their highly
6 confidential PII would be stored on Defendant’s networks.

7 7. By obtaining, collecting, using, and deriving a benefit from Plaintiff’s
8 and Class Members’ PII, Defendant assumed legal and equitable duties to Plaintiff
9 and the Class. These duties arose from state and federal statutes and regulations as
10 well as common law principles.

11 8. Defendant disregarded the rights of Plaintiff and Class Members by
12 intentionally, willfully, recklessly and/or negligently failing to take and implement
13 adequate and reasonable measures to ensure that Plaintiff’s and Class Members’ PII
14 was safeguarded, failing to take available steps to prevent an unauthorized disclosure
15 of data and failing to follow applicable, required and appropriate protocols, policies
16 and procedures regarding the encryption of data, even for internal use. As a result,
17 the PII of Plaintiff and Class Members was compromised through disclosure to an
18 unknown and unauthorized third party—an undoubtedly nefarious third party that
19 seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the
20 future.

21 9. Due to Toshiba’s negligent failure to secure and protect Plaintiff’s and
22 Class Members’ Private Information, cybercriminals have stolen and obtained
23 everything they need to commit identity theft and wreak havoc on the financial and
24 personal lives of millions of individuals.

25 10. Now, and for the rest of their lives, Plaintiff and the Class Members
26

27 ⁶ *Id.*

1 will have to deal with the danger of identity thieves possessing and misusing their
2 Private Information. Even those Class Members who have yet to experience identity
3 theft will have to spend time responding to the Data Breach and are at an immediate
4 and heightened risk of all manners of identity theft as a direct and proximate result
5 of the Data Breach.

6 11. Plaintiff and Class Members have incurred and will continue to incur
7 damages in the form of, among other things, identity theft, attempted identity theft,
8 lost time and expenses mitigating harms, increased risk of harm, damaged credit,
9 diminution of the value of their Private Information, loss of privacy, and additional
10 damages as described below.

11 12. Plaintiff and Class Members have a continuing interest in ensuring that
12 their information is and remains safe, and they are entitled to injunctive and other
13 equitable relief.

14 13. Plaintiff brings this action individually and on behalf of the Class,
15 seeking compensatory damages, punitive damages, nominal damages, restitution,
16 injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other
17 remedies this Court deems just and proper.

18 **II. THE PARTIES**

19 14. **Plaintiff Kyle McDaniel** is an individual domiciled in Cordova,
20 Tennessee. Plaintiff received a Notice of Data Breach Letter from Toshiba dated
21 July 23, 2024, notifying him that his name and Social Security number were
22 "accessible to the unauthorized individual" and compromised in the Data Breach.⁷

23 15. Defendant **Toshiba America Business Solutions, Inc.**, is a corporation
24 incorporated in California and with its principal place of business at 25530
25 Commercentre Drive, Lake Forest, California 92630.

26
27 ⁷ Ex. 1 (Notice of Data Breach Letter).

1 **III. JURISDICTION AND VENUE**

2 16. Jurisdiction is proper in this Court under 28 U.S.C. § 1332(d).
3 Specifically, this Court has subject matter and diversity jurisdiction over this action
4 under 28 U.S.C. § 1332(d) because this is a class action where the amount in
5 controversy exceeds the sum or value of \$5 million, exclusive of interest and costs,
6 there are more than 100 members in the proposed class and at least one other Class
7 Member is a citizen of a state different from Defendant.

8 17. Supplemental jurisdiction to adjudicate issues pertaining to state law is
9 proper in this Court under 28 U.S.C. § 1367.

10 18. As previously stated, Defendant is headquartered in this District and
11 has its principal place of business in this District. Defendant also has sufficient
12 minimum contacts in California and has intentionally availed itself of this
13 jurisdiction by marketing and selling products and services and by accepting and
14 processing payments for those products and services within California.

15 19. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1) because a
16 substantial part of the events that gave rise to Plaintiff's claims took place within
17 this District, and Defendant does business and has its headquarters and principal
18 place of business here.

19 **IV. FACTUAL ALLEGATIONS**

20 **A. Toshiba and its Collection of Plaintiff's and the Class's PII.**

21 20. Toshiba America Business Solutions is a subsidiary of Toshiba TEC
22 corporation and is known for its office printing and retail solutions across the United
23 States and Latin America.⁸

24 21. According to Zippia, Toshiba's annual revenue is approximately \$1.1
25

26
27 ⁸ <https://cybernews.com/news/toshiba-email-compromise-data-incident/>.

1 billion, and the company employs almost 4,000 people.⁹

2 22. Toshiba could have afforded to implement adequate data security prior
3 to the Breach but deliberately chose not to.

4 23. In the ordinary course of business, Toshiba receives the PII of
5 individuals, such as Plaintiff and the Class, through its customers and its current and
6 former employees.

7 24. Toshiba obtains, collects, uses, and derives a benefit from the PII of
8 Plaintiff and Class Members. Toshiba uses the PII it collects to provide services to
9 its clients, making a profit therefrom. Toshiba would not be able to obtain revenue
10 if not for the acceptance and use of Plaintiff's and the Class's PII.

11 25. By collecting Plaintiff's and the Class's PII, Toshiba assumed legal and
12 equitable duties to Plaintiff and the Class to protect and safeguard their PII from
13 unauthorized access and intrusion.

14 26. Toshiba recognizes this duty and makes the following claim on its
15 website regarding its protection of sensitive data: "Toshiba has implemented
16 technical and organizational security measures to provide reasonable security for
17 your Personal Information."¹⁰

18 27. Toshiba's assurances of maintaining high standards of cybersecurity
19 make it evident that Toshiba recognized it had a duty to use reasonable measures to
20 protect the PII that it collected and maintained.

21 28. Toshiba violated its own Privacy Policy and failed to adopt reasonable
22 and appropriate security practices and procedures including administrative, physical
23 security, and technical controls to safeguard Plaintiff's and the Class's Private
24 Information.

25
26 ⁹ *Id.*

27 ¹⁰ <https://business.toshiba.com/privacy-policy>.

29. As a result, Plaintiff's and Class Members' PII was accessed and stolen from Toshiba's inadequately secured email systems in a massive and preventable Data Breach.

B. Toshiba's Massive and Preventable Data Breach.

30. On an undisclosed date, Toshiba discovered suspicious activity within its email environment.¹¹

31. After detecting the Breach, Toshiba claims it initiated an investigation in which it determined cybercriminals infiltrated Toshiba's email environment between December 4, 2023, and March 18, 2024."¹²

32. Toshiba gives no explanation as to why the Data Breach was allowed to continue for so long or why Toshiba failed to detect the Breach until months after it initially began.

33. Toshiba claims investigation of the Data Breach is still ongoing, but on May 1, 2024, it learned that personal information was potentially viewed by an unauthorized individual.¹³

34. The Private Information accessed without authorization in the Data Breach included Social Security numbers and names.¹⁴

35. Despite the Data Breach beginning in December 2023, Toshiba did not begin notifying individuals of the Data Breach until May 28, 2024,¹⁵ with some not being notified until late July 2024.¹⁶

36. In recognition of the severity of the Data Breach, and the imminent risk

¹¹ <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/401acca4-7cb4-4d16-899b-82b4fabe9bf6.shtml>.

¹² *Id.*

¹³ *Id.*

¹⁴ *Id.*

¹⁵ *Id.*

¹⁶ *See* Ex. 1.

1 of harm Plaintiff and the Class face, Toshiba made an offering of twenty-four (24)
2 months of identity theft protection services. Such an offering is inadequate and will
3 not prevent identity theft but will only alert Data Breach victims once identity theft
4 has *already occurred*.

5 37. All in all, Toshiba failed to take the necessary precautions required to
6 safeguard and protect Plaintiff's and Class Members' PII from unauthorized access
7 and exploitation.

8 38. Defendant's actions represent a flagrant disregard of the rights of
9 Plaintiff and the Class, both as to privacy and property.

10 **C. Cyber Criminals Have Used and Will Continue to Use Plaintiff's and the**
11 **Class's PII to Defraud Them.**

12 39. PII is of great value to hackers and cybercriminals, and the data stolen
13 in the Data Breach can and will be used in a variety of ways by criminals to exploit
14 Plaintiff and the Class Members and to profit off their misfortune.

15 40. Each year, identity theft causes tens of billions of dollars of losses to
16 victims in the United States.¹⁷

17 41. For example, with the PII stolen in the Data Breach, including Social
18 Security numbers, identity thieves can open financial accounts, apply for credit, file
19 fraudulent tax returns, commit crimes, create false driver's licenses and other forms
20 of identification and sell them to other criminals or undocumented immigrants, steal
21 government benefits, give breach victims' names to police during arrests, and many
22
23
24

25 ¹⁷ *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST.,
26 <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>
27 (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters
a New Era of Complexity").

1 other harmful forms of identity theft.¹⁸ These criminal activities have and will result
2 in devastating financial and personal losses to Plaintiff and the Class Members.

3 42. Social security numbers are particularly sensitive pieces of personal
4 information. As the Consumer Federation of America explains:

5
6 **Social Security number.** *This is the most dangerous type of personal*
7 *information in the hands of identity thieves* because it can open the gate
8 to serious fraud, from obtaining credit in your name to impersonating
9 you to get medical services, government benefits, your tax refunds,
10 employment – even using your identity in bankruptcy and other legal
11 matters. It’s hard to change your Social Security number and it’s not a
12 good idea because it is connected to your life in so many ways.¹⁹
13 (Emphasis added).

14
15 43. PII is such a valuable commodity to identity thieves that once it has
16 been compromised, criminals will use it for years.²⁰

17 44. This was a financially motivated breach, as the only reason the
18 cybercriminals go through the trouble of running targeted cyberattacks against
19 companies like Toshiba is to get ransom money and/or information that they can
20

21
22 ¹⁸ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security*
23 *Number*, CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

24 ¹⁹ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF
25 AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

26 ²⁰ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;*
27 *However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at
<https://www.gao.gov/products/gao-07-737>.

1 monetize by selling on the black market for use in the kinds of criminal activity
2 described herein.

3 45. Indeed, a social security number, date of birth, and full name can sell
4 for \$60 to \$80 on the digital black market.²¹

5 46. “[I]f there is reason to believe that your personal information has been
6 stolen, you should assume that it can end up for sale on the dark web.”²²

7 47. These risks are both certainly impending and substantial. As the Federal
8 Trade Commission (“FTC”) has reported, if hackers get access to PII, ***they will use***
9 ***it***.²³

10 48. Hackers may not use the information right away, but this does not mean
11 it will not be used. According to the U.S. Government Accountability Office, which
12 conducted a study regarding data breaches:

13
14 [I]n some cases, stolen data may be held for up to a year or more before
15 being used to commit identity theft. Further, once stolen data have been
16 sold or posted on the Web, fraudulent use of that information ***may***
17 ***continue for years***. As a result, studies that attempt to measure the harm
18
19
20

21 ²¹ Michael Kan, *Here’s How Much Your Identity Goes for on the Dark Web* (Nov.
22 15, 2017), [https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-](https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web)
23 [on-the-dark-web](https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web).

24 ²² *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF
25 AMERICA (Mar. 19, 2019), [https://consumerfed.org/consumer_info/dark-web-](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/)
26 [monitoring-what-you-should-know/](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/).

27 ²³ Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER
28 (May 24, 2017), [https://www.militaryconsumer.gov/blog/how-fast-will-identity-](https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info)
[thieves-use-stolen-info](https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info).

1 resulting from data breaches cannot necessarily rule out all future
2 harm.²⁴

3 49. For instance, with a stolen social security number, which is part of the
4 PII compromised in the Data Breach, someone can open financial accounts, get
5 medical care, file fraudulent tax returns, commit crimes, and steal benefits.²⁵

6 50. With just a Social Security number, a criminal can (i) obtain credit cards
7 or loans; (ii) open a new bank account; (iii) empty existing bank accounts; (iv) get a
8 fraudulent driver's license; (v) receive medical care; (vi) open a phone account; (vii)
9 commit crimes that will show up on the victim's record; (viii) steal benefits and
10 Social Security checks; (ix) set up utilities; and file a fraudulent tax returns.²⁶

11 51. Identity thieves have already started to prey on the Toshiba Data Breach
12 victims, and we can anticipate that this will continue.

13 52. Identity theft victims must spend countless hours and large amounts of
14 money repairing the impact to their credit as well as protecting themselves in the
15 future.²⁷

16 53. Defendant's offer of two (2) years of identity monitoring to Plaintiff
17 and the Class is woefully inadequate and will not fully protect Plaintiff from the
18 damages and harm caused by its failures.

19
20 ²⁴ *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at
21 <https://www.gao.gov/products/gao-07-737>.

22 ²⁵ See, e.g., Christine DiGangi, *What Can You Do with a Stolen Social Security*
23 *Number*, CREDIT.COM (June 29, 2020), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/>.

24 ²⁶ <https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number>.

25 ²⁷ *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept.
26 2013), available at <https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf>.

1 54. The full scope of the harm has yet to be realized. There may be a time
2 lag between when harm occurs versus when it is discovered, and between when PII
3 is stolen and when it is used.

4 55. Once the twenty-four months have expired, Plaintiff and Class
5 Members will need to pay for their own identity theft protection and credit
6 monitoring for the rest of their lives due to Toshiba's gross negligence.

7 56. Furthermore, identity monitoring only alerts someone to the fact that
8 they have *already been the victim of identity theft* (i.e., fraudulent acquisition and
9 use of another person's PII)—it does not prevent identity theft.²⁸ Nor can an identity
10 monitoring service remove personal information from the dark web.²⁹

11 57. “The people who trade in stolen personal information [on the dark web]
12 won't cooperate with an identity theft service or anyone else, so it's impossible to
13 get the information removed, stop its sale, or prevent someone who buys it from
14 using it.”³⁰

15 58. As a direct and proximate result of the Data Breach, Plaintiff and the
16 Class have been damaged and have been placed at an imminent, immediate, and
17 continuing increased risk of harm from continued fraud and identity theft. Plaintiff
18 and the Class must now take the time and effort to mitigate the actual and potential
19 impact of the Data Breach on their everyday lives, including placing “freezes” and
20 “alerts” with credit reporting agencies, contacting their financial institutions, closing
21

22
23 ²⁸ See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*,
24 CNBC (Nov. 30, 2017, 9:00 AM), [https://www.cnbc.com/2017/11/29/credit-](https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html)
25 [monitoring-services-may-not-be-worth-the-cost.html](https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html).

26 ²⁹ *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF
27 AMERICA (Mar. 19, 2019), [https://consumerfed.org/consumer_info/dark-web-](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know)
28 [monitoring-what-you-should-know](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know).

³⁰ *Id.*

1 or modifying financial accounts, and closely reviewing and monitoring bank
2 accounts and credit reports for unauthorized activity for years to come.

3 59. Even more seriously is the identity restoration that Plaintiff and other
4 Class Members must go through, which can include spending countless hours filing
5 police reports, filling out IRS forms, Federal Trade Commission checklists,
6 Department of Motor Vehicle driver's license replacement applications, and calling
7 financial institutions to cancel fraudulent credit applications, to name just a few of
8 the steps Plaintiff and the Class must take.

9 60. Plaintiff and the Class have or will experience the following concrete
10 and particularized harms for which they are entitled to compensation, including:

- 11 a. Actual identity theft;
- 12 b. Trespass, damage to, and theft of their personal property including PII;
- 13 c. Improper disclosure of their PII;
- 14 d. The imminent and certainly impending injury flowing from potential
15 fraud and identity theft posed by their PII being placed in the hands of
16 criminals;
- 17 e. Loss of privacy suffered as a result of the Data Breach, including the
18 harm of knowing cyber criminals have their PII;
- 19 f. Ascertainable losses in the form of time taken to respond to identity
20 theft and attempt to restore identity, including lost opportunities and
21 lost wages from uncompensated time off from work;
- 22 g. Ascertainable losses in the form of out-of-pocket expenses and the
23 value of their time reasonably expended to remedy or mitigate the
24 effects of the Data Breach;
- 25 h. Ascertainable losses in the form of deprivation of the value of
26 Plaintiff's and Class Members' Private Information for which there is
27

1 a well-established and quantifiable national and international market;

2 i. The loss of use of and access to their credit, accounts, and/or funds;

3 j. Damage to their credit due to fraudulent use of their PII; and/or

4 k. Increased cost of borrowing, insurance, deposits, and the inability to
5 secure more favorable interest rates because of a reduced credit score.

6 61. Moreover, Plaintiff and Class Members have an interest in ensuring that
7 their Private Information, which remains in the possession of Defendant, is protected
8 from further breaches by the implementation of industry standard security measures
9 and safeguards. Defendant has shown itself wholly incapable of protecting
10 Plaintiff's and the Class's Private Information.

11 62. Plaintiff and Class Members also have an interest in ensuring that their
12 Private Information that was provided to Toshiba is removed from all of Toshiba's
13 servers, email systems, and files.

14 63. Defendant itself acknowledged the harm caused by the Data Breach
15 because it offered Plaintiff and Class Members woefully inadequate identity theft
16 repair and monitoring services. Twenty-four months of identity theft and repair and
17 monitoring is, however, inadequate to protect Plaintiff and Class Members from a
18 lifetime of identity theft risk.

19 64. Defendant further acknowledged that the Data Breach would cause
20 inconvenience to affected individuals and that financial harm would likely occur,
21 stating, "[w]e apologize for any inconvenience or concern this incident may have
22 caused you."³¹

23 65. Additionally, the Notice of Data Breach Letter sent to Plaintiff and
24 other Class Members recognized that Toshiba needed to improve its cyber security
25

26 ³¹ [https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/401acca4-7cb4-4d16-899b-82b4fabe9bf6.shtml)
27 [a1252b4f8318/401acca4-7cb4-4d16-899b-82b4fabe9bf6.shtml](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/401acca4-7cb4-4d16-899b-82b4fabe9bf6.shtml).

1 protocols, stating “[t]o help prevent a similar incident from occurring in the future,
2 we implemented additional measures to enhance the security of our email
3 environment.”³²

4 66. These enhanced protections should have been in place before the Data
5 Breach.

6 67. At Toshiba’s suggestion, Plaintiff are desperately trying to mitigate the
7 damage that Toshiba has caused them.

8 68. Given the kind of Private Information Toshiba made accessible to
9 hackers, however, Plaintiff are certain to incur additional damages. Because identity
10 thieves have their PII, Plaintiff and all Class Members will need to have identity
11 theft monitoring protection for the rest of their lives. Some may even need to go
12 through the long and arduous process of getting a new Social Security number, with
13 all the loss of credit and employment difficulties that come with a new number.³³

14 69. None of this should have happened because the Data Breaches were
15 entirely preventable.

16 **D. Defendant was Aware of the Risk of Cyberattacks.**

17 70. Data security breaches have dominated the headlines for the last two
18 decades. And it doesn’t take an IT industry expert to know it. The general public can
19
20
21
22
23

24 ³² *Id.*

25 ³³ *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10,
26 2022), [https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-](https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html)
27 [number-affect-your-credit.html](https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html).

1 tell you the names of some of the biggest cybersecurity breaches: Target,³⁴ Yahoo,³⁵
2 Marriott International,³⁶ Chipotle, Chili's, Arby's,³⁷ and others.³⁸

3 71. Data breaches have been on the rise for a number of years, and this
4 trend is not slowing down. The last year has been littered with thefts of sensitive
5 information. Data breaches have affected companies and organizations of all shapes,
6 sizes, and sectors.³⁹

7 72. Businesses operating in the technology sector, such as Toshiba, are a
8 "wealth of sensitive data," and are "prime targets for hackers seeking financial gain,
9 intellectual property theft, or simply to wreak havoc."⁴⁰

10 73. Major and well-publicized data breaches in the tech industry include:
11 Yahoo, Facebook, LinkedIn, Microsoft Exchange Server, and Solar Winds.⁴¹
12

13 ³⁴ Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and*
14 *Lessons Learned*, ZDNET (Feb. 2, 2015), [https://www.zdnet.com/article/anatomy-](https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/)
15 [of-the-target-data-breach-missed-opportunities-and-lessons-learned/](https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/).

16 ³⁵ Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*,
17 CSOONLINE.COM (Oct. 4, 2017),
[https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-](https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html)
18 [how-they-did-it.html](https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html).

19 ³⁶ Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE:
20 HASHEDOUT (Mar. 22, 2019), [https://www.thesslstore.com/blog/autopsying-the-](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/)
21 [marriott-data-breach-this-is-why-insurance-matters/](https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/) (last visited Oct. 9, 2023).

22 ³⁷ Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle,*
23 *Others*, CNET (Aug. 1, 2018, 12:58 PM), [https://www.cnet.com/news/fbi-nabs-](https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b)
24 [alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-](https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b)
25 [10aaa1b](https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b).

26 ³⁸ See, e.g., Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the*
27 *21st Century*, CSO ONLINE (Nov. 8, 2022),
[https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-](https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html)
28 [century.html](https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html).

³⁹ <https://tech.co/news/data-breaches-updated-list>.

⁴⁰ <https://www.offsec.com/blog/top-technology-sector-breaches-and-threats/>.

⁴¹ *Id.*

1 74. Toshiba should certainly have been aware, and indeed was aware, that
2 it was at risk of a data breach that could expose the PII that it collected and
3 maintained.

4 75. Toshiba was clearly aware of the risks it was taking and the harm that
5 could result from inadequate data security.

6 **E. Toshiba Could Have Prevented the Data Breaches.**

7 76. Data breaches are preventable.⁴² As Lucy Thompson wrote in the DATA
8 BREACH AND ENCRYPTION HANDBOOK, “In almost all cases, the data breaches that
9 occurred could have been prevented by proper planning and the correct design and
10 implementation of appropriate security solutions.”⁴³ She added that “[o]rganizations
11 that collect, use, store, and share sensitive personal data must accept responsibility
12 for protecting the information and ensuring that it is not compromised”⁴⁴

13 77. “Most of the reported data breaches are a result of lax security and the
14 failure to create or enforce appropriate security policies, rules, and procedures. . . .
15 Appropriate information security controls, including encryption, must be
16 implemented and enforced in a rigorous and disciplined manner so that a *data breach*
17 *never occurs*.”⁴⁵

18 78. In Data Breaches like these, many failures laid the groundwork for the
19 Breach.

20 79. The FTC has published guidelines that establish reasonable data
21 security practices for businesses.

23 ⁴² Lucy L. Thomson, “Despite the Alarming Trends, Data Breaches Are
24 Preventable,” *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed.,
25 2012), available at <https://lawcat.berkeley.edu/record/394088>.

26 ⁴³*Id.* at 17.

27 ⁴⁴*Id.* at 28.

28 ⁴⁵*Id.*

1 80. The FTC guidelines emphasize the importance of having a data security
2 plan, regularly assessing risks to computer systems, and implementing safeguards to
3 control such risks.⁴⁶

4 81. The FTC guidelines establish that businesses should protect the
5 confidential information that they keep; properly dispose of personal information
6 that is no longer needed; encrypt information stored on computer networks;
7 understand their network's vulnerabilities; and implement policies for installing
8 vendor-approved patches to correct security problems.

9 82. The FTC guidelines also recommend that businesses utilize an intrusion
10 detection system to expose a breach as soon as it occurs; monitor all incoming traffic
11 for activity indicating hacking attempts; watch for large amounts of data being
12 transmitted from the system; and have a response plan ready in the event of a breach.

13 83. According to information and belief, Toshiba failed to maintain many
14 reasonable and necessary industry standards necessary to prevent a data breach,
15 including the FTC's guidelines.

16 84. Upon information and belief, Toshiba also failed to meet the minimum
17 standards of any of the following frameworks: the NIST Cybersecurity Framework,
18 NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and
19 Authorization Management Program (FEDRAMP); or the Center for Internet
20 Security's Critical Security Controls (CIS CSC), which are well respected
21 authorities in reasonable cybersecurity readiness.

25 ⁴⁶ *Protecting Personal Information: A Guide for Business*, FTC, available at
26 [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
27 [personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

85. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁴⁷

86. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breaches, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

⁴⁷ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view>.

- 1 • Manage the use of privileged accounts based on the principle of least
2 privilege: no users should be assigned administrative access unless
3 absolutely needed; and those with a need for administrator accounts
4 should only use them when necessary.
- 5 • Configure access controls—including file, directory, and network
6 share permissions—with least privilege in mind. If a user only needs
7 to read specific files, the user should not have write access to those
8 files, directories, or shares.
- 9 • Disable macro scripts from office files transmitted via email.
10 Consider using Office Viewer software to open Microsoft Office
11 files transmitted via email instead of full office suite applications.
- 12 • Implement Software Restriction Policies (SRP) or other controls to
13 prevent programs from executing from common ransomware
14 locations, such as temporary folders supporting popular Internet
15 browsers or compression/decompression programs, including the
16 AppData/LocalAppData folder.
- 17 • Consider disabling Remote Desktop protocol (RDP) if it is not being
18 used.
- 19 • Use application whitelisting, which only allows systems to execute
20 programs known and permitted by security policy.
- 21 • Execute operating system environments or specific programs in a
22 virtualized environment.
- 23 • Categorize data based on organizational value and implement
24 physical and logical separation of networks and data for different
25 organizational units.⁴⁸

26 ⁴⁸ *Id.* at 3–4.
27

1 87. Further, to prevent and detect malware attacks, Defendant could and
2 should have implemented, as recommended by the United States Cybersecurity &
3 Infrastructure Security Agency, the following measures:

- 4 • **Update and patch your computer.** Ensure your applications and
5 operating systems (OSs) have been updated with the latest patches.
6 Vulnerable applications and OSs are the target of most ransomware
7 attacks....
- 8 • **Use caution with links and when entering website addresses.** Be
9 careful when clicking directly on links in emails, even if the sender
10 appears to be someone you know. Attempt to independently verify
11 website addresses (e.g., contact your organization's helpdesk, search
12 the internet for the sender organization's website or the topic
13 mentioned in the email). Pay attention to the website addresses you
14 click on, as well as those you enter yourself. Malicious website
15 addresses often appear almost identical to legitimate sites, often
16 using a slight variation in spelling or a different domain (e.g., .com
17 instead of .net)....
- 18 • **Open email attachments with caution.** Be wary of opening email
19 attachments, even from senders you think you know, particularly
20 when attachments are compressed files or ZIP files.
- 21 • **Keep your personal information safe.** Check a website's security
22 to ensure the information you submit is encrypted before you
23 provide it....
- 24 • **Verify email senders.** If you are unsure whether or not an email is
25 legitimate, try to verify the email's legitimacy by contacting the
26 sender directly. Do not click on any links in the email. If possible,
27

1 use a previous (legitimate) email to ensure the contact information
2 you have for the sender is authentic before you contact them.

- 3 • **Inform yourself.** Keep yourself informed about recent
4 cybersecurity threats and up to date on ransomware techniques. You
5 can find information about known phishing attacks on the Anti-
6 Phishing Working Group website. You may also want to sign up for
7 CISA product notifications, which will alert you when a new Alert,
8 Analysis Report, Bulletin, Current Activity, or Tip has been
9 published.
- 10 • **Use and maintain preventative software programs.** Install
11 antivirus software, firewalls, and email filters—and keep them
12 updated—to reduce malicious network traffic....⁴⁹

13 88. In addition, to prevent and detect ransomware attacks, including the
14 ransomware attack that resulted in the Data Breach, Defendant could and should
15 have implemented, as recommended by the Microsoft Threat Protection Intelligence
16 Team, the following measures:

- 17 • **Secure internet-facing assets**
 - 18 - Apply latest security updates
 - 19 - Use threat and vulnerability management
 - 20 - Perform regular audit; remove privileged credentials
- 21 • **Thoroughly investigate and remediate alerts**
 - 22 - Prioritize and treat commodity malware infections as
23 potential full compromise;

25 ⁴⁹ See Security Tip (ST19-001) Protecting Against Ransomware (original release
26 date Apr. 11, 2019), available at [https://www.cisa.gov/news-](https://www.cisa.gov/news-events/news/protecting-against-ransomware)
27 [events/news/protecting-against-ransomware](https://www.cisa.gov/news-events/news/protecting-against-ransomware).

- 1 • **Include IT Pros in security discussions**
 - 2 - Ensure collaboration among [security operations],
 - 3 [security admins], and [information technology] admins to
 - 4 configure servers and other endpoints securely;
- 5 • **Build credential hygiene**
 - 6 - Use [multifactor authentication] or [network level
 - 7 authentication] and use strong, randomized, just-in-time
 - 8 local admin passwords
- 9 • **Apply principle of least-privilege**
 - 10 - Monitor for adversarial activities
 - 11 - Hunt for brute force attempts
 - 12 - Monitor for cleanup of Event Logs
 - 13 - Analyze logon events
- 14 • **Harden infrastructure**
 - 15 - Use Windows Defender Firewall
 - 16 - Enable tamper protection
 - 17 - Enable cloud-delivered protection
 - 18 - Turn on attack surface reduction rules and [Antimalware
 - 19 Scan Interface] for Office [Visual Basic for
 - 20 Applications].⁵⁰

21 89. Given that Defendant was storing the PII of tons of individuals,
22 Defendant could have and should have implemented all of the above measures to
23 prevent and detect cyberattacks.

25 ⁵⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020),
26 *available at* [https://www.microsoft.com/security/blog/2020/03/05/human-](https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/)
27 *operated-ransomware-attacks-a-preventable-disaster/*.

1 90. Specifically, among other failures, Toshiba had far too much
2 confidential unencrypted information held on its systems. Such PII should have
3 been segregated into an encrypted system.⁵¹

4 91. Moreover, it is well-established industry standard practice for a
5 business to dispose of confidential PII once it is no longer needed.

6 92. The FTC, among others, has repeatedly emphasized the importance of
7 disposing unnecessary PII, saying simply: “Keep sensitive data in your system only
8 as long as you have a business reason to have it. Once that business need is over,
9 properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”⁵²
10 Toshiba, rather than following this basic standard of care, kept thousands of
11 individuals’ unencrypted PII indefinitely.

12 93. In sum, these Data Breaches could have readily been prevented through
13 the use of industry standard network segmentation and encryption of all PII.

14 94. Further, the scope of the Data Breaches could have been dramatically
15 reduced had Toshiba utilized proper record retention and destruction practices.

16 **F. Plaintiff’s Individual Experience**

17 ***Plaintiff Kyle McDaniel***

18 95. Plaintiff McDaniel received a Notice of Data Breach Letter from
19 Defendant informing him that his highly confidential Private Information was
20 compromised in the Data Breach.

21 96. Plaintiff McDaniel is a former employee of Toshiba.
22

23 ⁵¹ See, e.g., Adnan Raja, *How to Safeguard Your Business Data with Encryption*,
24 FORTRA (Aug. 14, 2018), [https://digitalguardian.com/blog/how-safeguard-your-](https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption)
business-data-encryption.

25 ⁵² *Protecting Personal Information: A Guide for Business*, FTC, available at
26 [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
personal-information.pdf, at p. 6.
27

1 97. Defendant was in possession of Plaintiff's Private Information before,
2 during, and after the Data Breach.

3 98. Because of the Data Breach, there is no doubt Plaintiff McDaniel's
4 highly confidential Private Information is in the hands of cybercriminals. Reason
5 being, the Notice of Data Breach Letter from Defendant disclosed that an
6 unauthorized third-party had accessed Defendant's systems. The *modus operandi* of
7 cybercriminals involves stealing Private Information for financial gain.
8 Cybercriminals may use stolen identities to conceal their own true identity or carry
9 out a range of fraudulent activities, from credit card fraud to impersonation. As such,
10 Plaintiff McDaniel and the Class are at an imminent risk of identity theft and fraud.

11 99. As a result of the Data Breach, Plaintiff McDaniel has already expended
12 over **80 hours** of his time and has suffered loss of productivity from taking time to
13 address and attempt to ameliorate, mitigate, and address the future consequences of
14 the Data Breach. This includes: (i) investigating the Data Breach; (ii) investigating
15 how best to ensure that he is protected from identity theft; (iii) reviewing his account
16 statements, credit reports, and/or other information; and (iv) mitigating the fraud and
17 identity theft he has already experienced.

18 100. Plaintiff McDaniel has already suffered misuse of his Private
19 Information as a result of the Data Breach. On June 9, 2024, Plaintiff McDaniel
20 received a letter from Chase Bank informing him that someone was fraudulently
21 using his personal information and attempted to open an account in his name. In
22 response, Plaintiff McDaniel placed a fraud alert on his credit with Experian,
23 Equifax, and TransUnion and also "freezed" his credit. Plaintiff McDaniel estimates
24 he has spent at least 24 hours remedying the fraud he experienced.

25 101. Plaintiff McDaniel places significant value in the security of his Private
26 Information and does not readily disclose it. Plaintiff McDaniel has never
27
28

1 knowingly transmitted unencrypted Private Information over the internet or any
2 other unsecured source.

3 102. Plaintiff McDaniel has been and will continue to be at a heightened and
4 substantial risk of future identity theft and its attendant damages for years to come.
5 Such a risk is certainly real and impending, and is not speculative, given the highly
6 sensitive nature of the Private Information compromised by the Data Breach. Indeed,
7 Defendant acknowledged the present and increased risk of future harm Plaintiff
8 McDaniel and the Class now face by offering temporary, non-automatic credit
9 monitoring services to Plaintiff McDaniel and the Class.

10 103. Knowing that thieves intentionally targeted and stole his Private
11 Information, including his Social Security number, and knowing that his Private
12 Information is in the hands of cybercriminals has caused Plaintiff McDaniel great
13 anxiety beyond mere worry. Specifically, Plaintiff McDaniel has lost hours of sleep,
14 is in a constant state of stress, is very frustrated, and is in a state of persistent worry
15 now that his Private Information has been stolen.

16 104. Plaintiff McDaniel has a continuing interest in ensuring that his Private
17 Information, which, upon information and belief, remains in the possession of
18 Defendant, is protected, and safeguarded from future data breaches. Absent Court
19 intervention, Plaintiff's and the Class's Private Information will be wholly
20 unprotected and at-risk of future data breaches.

21 105. Plaintiff McDaniel has suffered injuries directly and proximately
22 caused by the Data Breach, including: (i) theft of his valuable Private Information;
23 (ii) the imminent and certain impending injury flowing from anticipated fraud and
24 identity theft posed by his Private Information being placed in the hands of
25 cybercriminals; (iii) damages to and diminution in value of his Private Information
26 that was entrusted to Defendant with the understanding that Defendant would
27

1 safeguard this information against disclosure; (iv) loss of the benefit of the bargain
2 with Defendant to provide adequate and reasonable data security—*i.e.*, the
3 difference in value between what Plaintiff McDaniel should have received from
4 Defendant and Defendant’s defective and deficient performance of that obligation
5 by failing to provide reasonable and adequate data security and failing to protect his
6 Private Information; and (v) continued risk to his Private Information, which remains
7 in the possession of Defendant and which is subject to further breaches so long as
8 Defendant fails to undertake appropriate and adequate measures to protect the
9 Private Information that was entrusted to Defendant.

10 **V. CLASS ACTION ALLEGATIONS**

11 106. Plaintiff incorporates by reference all preceding paragraphs as if fully
12 restated here.

13 107. Plaintiff brings this action against Toshiba on behalf of himself and all
14 other individuals similarly situated under Federal Rule of Civil Procedure 23.
15 Plaintiff asserts all claims on behalf of a nationwide class (the “Class”) defined as
16 follows:

17 **All persons who were sent a Notice of Data Breach**
18 **Letter from Toshiba after the Data Breach.**

19
20 108. Excluded from the Class are Defendant, any entity in which Defendant
21 has a controlling interest, and Defendant’s officers, directors, legal representatives,
22 successors, subsidiaries, and assigns. Also excluded from the Class is any judge,
23 justice, or judicial officer presiding over this matter and members of their immediate
24 families and judicial staff.

25 109. Plaintiff reserves the right to amend the above definition or to propose
26 subclasses in subsequent pleadings and motions for class certification.

1 110. Plaintiff anticipates the issuance of notice setting forth the subject and
2 nature of the instant action to the proposed Class. Upon information and belief,
3 Defendant's own business records or electronic media can be utilized for the notice
4 process.

5 111. The proposed Class meets the requirements of Federal Rule of Civil
6 Procedure 23.

7 112. **Numerosity:** The proposed Class is so numerous that joinder of all
8 members is impracticable.

9 113. **Typicality:** Plaintiff's claims are typical of the claims of the Class.
10 Plaintiff and all members of the Class were injured through Toshiba's uniform
11 misconduct. Toshiba's inadequate data security gave rise to Plaintiff's claims and
12 are identical to those that give rise to the claims of every other Class member because
13 Plaintiff and each member of the Class had their sensitive PII compromised in the
14 same way by the same conduct of Toshiba.

15 114. **Adequacy:** Plaintiff is an adequate representative of the Class because
16 Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has
17 retained counsel competent and highly experienced in data breach class action
18 litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action
19 vigorously. The interests of the Class will be fairly and adequately protected by
20 Plaintiff and their counsel.

21 115. **Superiority:** A class action is superior to other available means of fair
22 and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered
23 by each individual class member is relatively small in comparison to the burden and
24 expense of individual prosecution of complex and expensive litigation. It would be
25 very difficult if not impossible for members of the Class individually to effectively
26 redress Toshiba's wrongdoing. Even if Class members could afford such individual
27

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 benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

116. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

- a. Whether Defendant engaged in the wrongful conduct alleged herein;
- b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's PII;
- c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;
- d. Whether Toshiba breached its duties to Plaintiff and the Class;
- e. Whether Toshiba failed to provide adequate cyber security;
- f. Whether Toshiba knew or should have known that its computer and network security systems were vulnerable to cyber attacks;
- g. Whether Toshiba's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;
- h. Whether Toshiba was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network;
- i. Whether Toshiba was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breaches to include former employees and business associates;

- 1 j. Whether Toshiba breached implied contractual duties to Plaintiff and
2 the Class to use reasonable care in protecting their PII;
- 3 k. Whether Toshiba failed to adequately respond to the Data Breach,
4 including failing to investigate it diligently and notify affected
5 individuals in the most expedient time possible and without
6 unreasonable delay, and whether this caused damages to Plaintiff and
7 the Class;
- 8 l. Whether Toshiba continues to breach duties to Plaintiff and the Class;
- 9 m. Whether Plaintiff and the Class suffered injury as a proximate result of
10 Toshiba's negligent actions or failures to act;
- 11 n. Whether Plaintiff and the Class are entitled to recover damages,
12 equitable relief, and other relief; and
- 13 o. Whether Toshiba's actions alleged herein constitute gross negligence,
14 and whether Plaintiff and Class Members are entitled to punitive
15 damages.

16 **I. CAUSES OF ACTION**

17 **FIRST CAUSE OF ACTION**

18 **NEGLIGENCE**

19 **(On Behalf of Plaintiff and the Class)**

20 117. Plaintiff incorporates paragraphs 1–116 as though fully set forth herein.

21 118. Toshiba solicited, gathered, and stored the PII of Plaintiff and Class
22 Members.

23 119. Upon accepting and storing the PII of Plaintiff and Class members on
24 its computer systems and networks, Defendant undertook and owed a duty to
25 Plaintiff and Class members to exercise reasonable care in obtaining, retaining,
26 securing, safeguarding, deleting, and protecting the PII of Plaintiff and the Class
27

1 from being compromised, lost, stolen, accessed, and misused by unauthorized
2 persons.

3 120. Defendant had full knowledge of the sensitivity of the PII and the types
4 of harm that Plaintiff and Class members could and would suffer if the PII was
5 wrongfully disclosed. Plaintiff and Class members were the foreseeable victims of
6 any inadequate safety and security practices. Plaintiff and the Class members had no
7 ability to protect their PII that was in Defendant's possession. As such, a special
8 relationship existed between Defendant and Plaintiff and the Class.

9 121. Because of this special relationship, Defendant required Plaintiff and
10 Class members to provide their PII, including names, Social Security numbers, and
11 other PII.

12 122. Implied in these exchanges was a promise by Defendant to ensure that
13 the PII of Plaintiff and Class members in its possession was only used for the
14 provided purpose and that Defendant would destroy any PII that it was not required
15 to maintain.

16 123. As part of this special relationship, Defendant had a duty to perform
17 with skill, care, and reasonable expedience and faithfulness.

18 124. Through Defendant's acts and omissions, including Defendant's failure
19 to provide adequate data security, its failure to protect Plaintiff's and Class
20 members' PII from being foreseeably accessed, and its improper retention of PII it
21 was not required to maintain, Defendant negligently failed to observe and perform
22 its duty.

23 125. Plaintiff and Class members did not receive the benefit of the bargain
24 with Defendant, because providing their PII was in exchange for Defendant's
25 implied agreement to secure and keep it safe and to delete it once no longer required.
26
27
28

1 126. Defendant was aware of the fact that cybercriminals routinely target
2 large corporations through cyberattacks in an attempt to steal customer and
3 employee PII. In other words, Defendant knew of a foreseeable risk to its data
4 security systems but failed to implement reasonable security measures.

5 127. Defendant owed Plaintiff and the Class members a common law duty
6 to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the
7 Class when obtaining, storing, using, and managing personal information, including
8 taking action to reasonably safeguard or delete such data and providing notification
9 to Plaintiff and the Class members of any breach in a timely manner so that
10 appropriate action could be taken to minimize losses.

11 128. Defendant's duty extended to protecting Plaintiff and the Class from
12 the risk of foreseeable criminal conduct of third parties, which has been recognized
13 in situations where the actor's own conduct or misconduct exposes another to the
14 risk or defeats protections put in place to guard against the risk, or where the parties
15 are in a special relationship. *See* Restatement (Second) of Torts § 302B.

16 129. Defendant had duties to protect and safeguard the PII of Plaintiff and
17 the Class from being vulnerable to cyberattacks by taking common-sense
18 precautions when dealing with sensitive PII. Additional duties that Defendant owed
19 Plaintiff and the Class include:

- 20 a. To exercise reasonable care in designing, implementing, maintaining,
21 monitoring, and testing Defendant's networks, systems, protocols,
22 policies, procedures and practices to ensure that Plaintiff's and Class
23 members' PII was adequately secured from impermissible release,
24 disclosure, and publication;
- 25 b. To protect Plaintiff's and Class members' PII in its possession by using
26 reasonable and adequate security procedures and systems;
- 27

- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and
- d. To promptly notify Plaintiff and Class members of any data breach, security incident, or intrusion that affected or may have affected their PII.

130. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and Defendant. Defendant was in a position to ensure that its systems were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

131. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

132. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class members' PII. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, and protecting the PII in its possession;
- b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;
- c. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's PII;
- d. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;
- e. Failing to promptly notify Plaintiff and Class members of the Data Breaches that affected their PII.

133. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

1 134. As a direct and proximate result of Defendant's negligent conduct,
2 including but not limited to its failure to implement and maintain reasonable data
3 security practices and procedures as described above, Plaintiff and the Class have
4 suffered damages and are at imminent risk of additional harms and damages (as
5 alleged above).

6 135. Through Defendant's acts and omissions described herein, including
7 but not limited to Defendant's failure to protect the PII of Plaintiff and Class
8 members from being stolen and misused, Defendant unlawfully breached its duty to
9 use reasonable care to adequately protect and secure the PII of Plaintiff and Class
10 members while it was within Defendant's possession and control.

11 136. Further, through its failure to provide timely and clear notification of
12 the Data Breach to Plaintiff and Class members, Defendant prevented Plaintiff and
13 Class members from taking meaningful, proactive steps to securing their PII and
14 mitigating damages.

15 137. Plaintiff and Class members could have taken actions earlier had they
16 been timely notified of the Data Breach, rather than months after it occurred.

17 138. Plaintiff and Class members could have enrolled in credit monitoring,
18 could have instituted credit freezes, and could have changed their passwords, among
19 other things, had they been alerted to the Data Breach more quickly.

20 139. Plaintiff and Class members have suffered harm from the delay in
21 notifying them of the Data Breach.

22 140. As a direct and proximate cause of Defendant's conduct, including but
23 not limited to its failure to implement and maintain reasonable security practices and
24 procedures, Plaintiff and Class members have suffered, as Plaintiff have, and/or will
25 suffer injury and damages, including but not limited to: (i) the loss of the opportunity
26 to determine for themselves how their PII is used; (ii) the publication and/or theft of
27

1 their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and
2 recovery from identity theft, tax fraud, and/or unauthorized use of their PII,
3 including the need for substantial credit monitoring and identity protection services
4 for an extended period of time; (iv) lost opportunity costs associated with effort
5 expended and the loss of productivity addressing and attempting to mitigate the
6 actual and future consequences of the Data Breaches, including but not limited to
7 efforts spent researching how to prevent, detect, contest and recover from tax fraud
8 and identity theft; (v) costs associated with placing freezes on credit reports and
9 password protections; (vi) anxiety, emotional distress, loss of privacy, and other
10 economic and non-economic losses; (vii) the continued risk to their PII, which
11 remains in Defendant's possession and is subject to further unauthorized disclosures
12 so long as Defendant fails to undertake appropriate and adequate measures to protect
13 the PII of employees in its continued possession; and, (viii) future costs in terms of
14 time, effort and money that will be expended to prevent, detect, contest, and repair
15 the inevitable and continuing consequences of compromised PII for the rest of their
16 lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven
17 at trial.

18 141. The damages Plaintiff and the Class have suffered (as alleged above)
19 and will suffer were and are the direct and proximate result of Defendant's negligent
20 conduct.

21 142. Plaintiff and the Class have suffered injury and are entitled to actual
22 and punitive damages in an amount to be proven at trial.

23 **SECOND CAUSE OF ACTION**

24 **NEGLIGENCE *PER SE***

25 **(On Behalf of Plaintiff and the Class)**

26 143. Plaintiff incorporates paragraphs 1–116 as though fully set forth herein.
27

1 144. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to
2 Plaintiff and the Class to provide fair and adequate computer systems and data
3 security to safeguard the PII of Plaintiff and the Class.

4 145. The FTC Act prohibits “unfair practices in or affecting commerce,”
5 including, as interpreted and enforced by the FTC, the unfair act or practice by
6 businesses, such as Defendant, of failing to use reasonable measures to protect PII.
7 The FTC publications and orders described above also formed part of the basis of
8 Defendant’s duty in this regard.

9 146. Defendant gathered and stored the PII of Plaintiff and the Class as part
10 of its business which affects commerce.

11 147. Defendant violated the FTC Act by failing to use reasonable measures
12 to protect the PII of Plaintiff and the Class and by not complying with applicable
13 industry standards, as described herein.

14 148. Defendant breached its duties to Plaintiff and the Class under the FTC
15 Act by failing to provide fair, reasonable, or adequate computer systems and/or data
16 security practices to safeguard Plaintiff’s and Class members’ PII, and by failing to
17 provide prompt notice without reasonable delay.

18 149. Defendant’s multiple failures to comply with applicable laws and
19 regulations constitutes negligence *per se*.

20 150. Plaintiff and the Class are within the class of persons that the FTC Act
21 was intended to protect.

22 151. The harm that occurred as a result of the Data Breach is the type of
23 harm the FTC Act was intended to guard against.

24 152. Defendant breached its duties to Plaintiff and the Class under the FTC
25 Act by failing to provide fair, reasonable, or adequate computer systems and data
26 security practices to safeguard Plaintiff’s and the Class’s PII.

1 other things, failing to (i) use reasonable data security measures, (ii) implement
2 adequate protocols and employee training sufficient to protect Plaintiff's and Class
3 Members' Private Information from unauthorized disclosure to third parties, and (iii)
4 promptly and adequately notify Plaintiff and Class Members of the Data Breach.

5 163. Plaintiff and the Class were harmed by Defendant's breaches of
6 contract, as such breach is alleged herein, and are entitled to the losses and damages
7 they have sustained as a direct and proximate result thereof.

8 164. Plaintiff and Class Members are also entitled to their costs and
9 attorney's fees incurred in this action.

10 **FOURTH CAUSE OF ACTION**

11 **UNJUST ENRICHMENT**

12 **(On Behalf of Plaintiff and the Class)**

13 165. Plaintiff incorporates paragraphs 1–116 as though fully set forth herein.

14 166. Plaintiff alleges this claim in the alternative to his breach of implied
15 contract claim.

16 167. Defendant knew that Plaintiff and Class Members conferred a benefit
17 upon it and accepted and retained that benefit by accepting and retaining the PII
18 entrusted to it. Defendant profited from Plaintiff's retained data and commercialized
19 and used Plaintiff's and Class Members' PII for business purposes.

20 168. Upon information and belief, Defendant funds its data security
21 measures entirely from its general revenue, including payments on behalf of or for
22 the benefit of Plaintiff and Class Members.

23 169. As such, a portion of the payments made for the benefit of or on behalf
24 of Plaintiff and Class Members is to be used to provide a reasonable level of data
25 security, and the amount of the portion of each payment made that is allocated to
26 data security is known to Defendant.

1 170. Defendant failed to secure Plaintiff's and Class Members' Private
2 Information and, therefore, did not fully compensate Plaintiff or Class Members for
3 the value that their PII provided.

4 171. Defendant acquired the PII through inequitable means as it failed to
5 disclose the inadequate data security practices previously alleged. If Plaintiff and
6 Class Members had known that Defendant would not fund adequate data security
7 practices, procedures, and protocols to sufficiently monitor, supervise, and secure
8 their PII, they would not have entrusted their Private Information to Defendant or
9 obtained services from Defendant's clients.

10 172. Defendant enriched itself by saving the costs it reasonably should have
11 expended on data security measures to secure Plaintiff's and Class Members' PII.
12 Instead of providing a reasonable level of security that would have prevented the
13 Data Breach, Defendant instead calculated to increase its own profits at the expense
14 of Plaintiff and Class Members by utilizing cheaper, ineffective security measures
15 and diverting those funds to their own benefit. Plaintiff and Class Members, on the
16 other hand, suffered as a direct and proximate result of Defendant's decision to
17 prioritize its own profits over the requisite security and the safety of their PII.

18 173. Plaintiff and Class Members have no adequate remedy at law.

19 174. Under the circumstances, it would be unjust for Defendant to be
20 permitted to retain any of the benefits that Plaintiff and Class Members conferred
21 upon it.

22 175. As a direct and proximate result of Defendant's conduct, Plaintiff and
23 other Class Members, have suffered actual harm in the form of experiencing specific
24 acts of fraudulent activity and other attempts of fraud that required Plaintiff's efforts
25 to prevent from succeeding.

1 176. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff
2 and the Class are entitled to restitution and disgorgement of profits, benefits, and
3 other compensation obtained by Defendant and all other relief allowed by law.

4 **FIFTH CAUSE OF ACTION**

5 **DECLARATORY AND INJUNCTIVE RELIEF**

6 **(On Behalf of Plaintiff and the Class)**

7 177. Plaintiff incorporates paragraphs 1–116 as though fully set forth herein.

8 178. This count is brought under the Federal Declaratory Judgment Act, 28
9 U.S.C. § 2201.

10 179. As previously alleged, Plaintiff and members of the Class are entered
11 into implied contracts with Defendant, which contracts required Defendant to
12 provide adequate security for the PII collected from Plaintiff and the Class.

13 180. Defendant owed and still owes a duty of care to Plaintiff and Class
14 members that require it to adequately secure Plaintiff's and Class members' PII.

15 181. Upon reason and belief, Defendant still possesses the PII of Plaintiff
16 and the Class members.

17 182. Defendant has not satisfied its contractual obligations and legal duties
18 to Plaintiff and the Class members.

19 183. Since the Data Breach, Defendant has not yet announced any changes
20 to its data security infrastructure, processes or procedures to fix the vulnerabilities
21 in its computer systems and/or security practices which permitted the Data Breach
22 to occur and go undetected and, thereby, prevent further attacks.

23 184. Defendant has not satisfied its contractual obligations and legal duties
24 to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is
25 known to hackers, the PII in Defendant's possession is even more vulnerable to
26 cyberattack.

1 185. Actual harm has arisen in the wake of the Data Breach regarding
2 Defendant's contractual obligations and duties of care to provide security measures
3 to Plaintiff and the members of the Class. Further, Plaintiff and the members of the
4 Class are at risk of additional or further harm due to the exposure of their PII and
5 Defendant's failure to address the security failings that led to such exposure.

6 186. There is no reason to believe that Defendant's security measures are
7 any more adequate now than they were before the Data Breaches to meet
8 Defendant's contractual obligations and legal duties.

9 187. Plaintiff and the Class, therefore, seek a declaration (1) that
10 Defendant's existing security measures do not comply with its contractual
11 obligations and duties of care to provide adequate security, and (2) that to comply
12 with its contractual obligations and duties of care, Defendant must implement and
13 maintain reasonable security measures, including, but not limited to:

- 14 a. Ordering that Defendant engage third-party security
15 auditors/penetration testers as well as internal security personnel to
16 conduct testing, including simulated attacks, penetration tests, and
17 audits on Defendant's systems on a periodic basis, and ordering
18 Defendant to promptly correct any problems or issues detected by
19 such third-party security auditors;
- 20 b. Ordering that Defendant engage third-party security auditors and
21 internal personnel to run automated security monitoring;
- 22 c. Ordering that Defendant audit, test, and train its security personnel
23 regarding any new or modified procedures;
- 24 d. Ordering that Defendant segment employee data by, among other
25 things, creating firewalls and access controls so that if one area of
26 Defendant's systems is compromised, hackers cannot gain access to
27

1 other portions of Defendant's systems;

2 e. Ordering that Defendant purge, delete, and destroy, in a reasonably
3 secure manner, customer data not necessary for their provisions of
4 services;

5 f. Ordering that Defendant conduct regular database scanning and
6 security checks; and

7 g. Ordering that Defendant routinely and continually conduct internal
8 training and education to inform internal security personnel how to
9 identify and contain a breach when it occurs and what to do in
10 response to a breach.

11 **VI. PRAYER FOR RELIEF**

12 WHEREFORE, Plaintiff and the Class pray for judgment against Defendant
13 as follows:

14 a. An order certifying this action as a class action under Federal Rule
15 of Civil Procedure 23, defining the Class as requested herein,
16 appointing the undersigned as Class counsel, and finding that
17 Plaintiff are proper representatives of the Class requested herein;

18 b. A judgment in favor of Plaintiff and the Class awarding them
19 appropriate monetary relief, including compensatory damages,
20 punitive damages, attorney fees, expenses, costs, and such other and
21 further relief as is just and proper;

22 c. An order providing injunctive and other equitable relief as necessary
23 to protect the interests of the Class as requested herein;

24 d. An order requiring Defendant to pay the costs involved in notifying
25 the Class Members about the judgment and administering the claims
26 process;

- 1 e. A judgment in favor of Plaintiff and the Class awarding them pre-
2 judgment and post-judgment interest, reasonable attorneys' fees,
3 costs, and expenses as allowable by law; and
4 f. An award of such other and further relief as this Court may deem
5 just and proper.

6 **II. DEMAND FOR JURY TRIAL**

7 Plaintiff hereby demands a trial by jury on all appropriate issues raised in this
8 Class Action Complaint.

9 Dated: August 13, 2024

Respectfully submitted,

10
11 /s/: Byron T. Ball

Byron T. Ball

(State Bar No. 150195)

THE BALL LAW FIRM APC

100 Wilshire Blvd., Suite 700

Santa Monica, CA 90401

Telephone: (310) 980-8039

Facsimile: (415) 477-6710

Email: btb@balllawllp.com

17 William B. Federman

18 (*pro hac vice application forthcoming*)

19 Kennedy M. Brian

(*pro hac vice application forthcoming*)

FEDERMAN & SHERWOOD

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

T: (405) 235-1560

F: (405) 239-2112

E: wbf@federmanlaw.com

E: kpb@federmanlaw.com

EXHIBIT 1



TOSHIBA



4_0000861

July 23, 2024

KYLE MCDANIEL


Dear Kyle-Mcdaniel:

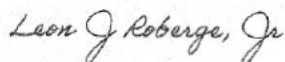
Toshiba Global Commerce Solutions, Inc. is committed to protecting the confidentiality and security of the personal information we maintain. I am writing to inform you of a data security incident that potentially involved some of your information. This notice explains the incident, the measures we have taken, and some steps you may consider taking in response.

We identified and addressed suspicious activity within our email environment. When we first learned of this activity, we immediately took steps to ensure our email tenant was secure. The investigation into the full scope of the incident is ongoing; however, based upon our preliminary review, your name and Social Security number were accessible to an unauthorized individual.

We arranged for you to receive a complimentary, two-year membership of identity monitoring services through Kroll. This product includes triple bureau credit monitoring, fraud consultation, and identity theft restoration. These services are completely free to you and activating these services will not hurt your credit score. For more information on identity theft prevention, additional steps you can take in response, and instructions on how to activate your complimentary, two-year membership, please see the information provided with this letter.

We regret any inconvenience or concern this incident may have caused you. To help prevent a similar incident from occurring in the future, we implemented additional measures to enhance the security of our email environment. If you have any questions about the incident, please feel free to contact our dedicated helpline at (866) 810-5653 from 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding certain U.S. holidays.

Sincerely,



Leon Roberge, Jr.
Chief Information Officer | Toshiba Global Commerce Solutions, Inc.