

1 William B. Federman (*pro hac vice*)  
2 Kennedy M. Brian (*pro hac vice*)  
3 **FEDERMAN & SHERWOOD**  
4 10205 N. Pennsylvania Ave.  
5 Oklahoma City, OK 73120  
6 T: (405) 235-1560  
7 F: (405) 239-2112  
8 E: wbf@federmanlaw.com  
9 E: kpb@federmanlaw.com  
10 *Attorneys for Plaintiffs and Proposed Class*  
11 *Additional Counsel on Signature Page*

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

15 **KYLE MCDANIEL, RIKKI**  
16 **MCDANIEL, JON WILLIAMS, and**  
17 **MOJDEH WILLIAMS, on behalf of**  
18 themselves and all similarly situated  
19 individuals,

20 Plaintiffs,

21 v.

22 **TOSHIBA GLOBAL COMMERCE**  
23 **SOLUTIONS and TOSHIBA**  
24 **AMERICA BUSINESS**  
25 **SOLUTIONS, INC.,**

26 Defendants.

Case No.: 8:24-cv-01772

**FIRST AMENDED**  
**CLASS ACTION COMPLAINT**

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

**JURY TRIAL DEMANDED**

27 Plaintiffs Kyle McDaniel, Rikki McDaniel, Jon Williams, and Mojdeh  
28 Williams (collectively, "Plaintiffs"), individually and on behalf of all other similarly  
situated individuals (the "Class" or "Class Members," as defined below), by and  
through their undersigned counsel, file this First Amended Class Action Complaint

1 against Toshiba America Business Solutions, Inc. (“TABS”) and Toshiba Global  
2 Commerce Solutions (“TGCS”) (collectively, “Toshiba” or “Defendants”) and  
3 allege the following based on personal knowledge of facts, upon information and  
4 belief, and based on the investigation of their counsel as to all other matters.

## 5 **I. INTRODUCTION**

6 1. Plaintiffs bring this class action lawsuit against Toshiba for its failure  
7 to protect Plaintiffs’ and the Class’s highly sensitive personally identifiable  
8 information (“PII”) from hackers.<sup>1</sup> As a result of Toshiba’s inadequate data security,  
9 cybercriminals easily infiltrated Defendants’ inadequately protected email accounts  
10 and accessed the PII of Plaintiffs and the Class (the “Data Breach” or “Breach”).<sup>2</sup>  
11 Now, Plaintiffs’ and the Class’s PII is in the hands of cybercriminals who will sell  
12 their PII on the dark web and use their PII for nefarious purposes for the rest of their  
13 lives.

14 2. On an undisclosed date, Toshiba discovered suspicious activity within  
15 its email environment.<sup>3</sup> After an investigation, it was determined that an unknown  
16 and unauthorized threat actor hacked into Toshiba’s inadequately secured email  
17 environment between December 4, 2023, through March 18, 2024. Thus, the  
18 hacker(s) had access to Toshiba’s email accounts—and Plaintiffs’ and the Class’s  
19 PII contained therein—for *over three (3) months*.<sup>4</sup>

---

21 <sup>1</sup> OFFICE OF THE MAINE ATTORNEY GENERAL, *Toshiba America Business Solutions*,  
22 [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)  
23 [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) (last visited Dec. 7,  
24 2024); OFFICE OF THE MAINE ATTORNEY GENERAL, *Toshiba Global Commerce*  
25 *Solutions*, [https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8feal1aeb-d918-4c0d-b40d-97990f1eb395.html)  
26 [a1252b4f8318/8feal1aeb-d918-4c0d-b40d-97990f1eb395.html](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8feal1aeb-d918-4c0d-b40d-97990f1eb395.html) (last visited Dec. 7,  
27 2024).

28 <sup>2</sup> *Id.*

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

1           3.     Toshiba claims the investigation of the Data Breach is still ongoing, but  
2 after a preliminary review Toshiba has already determined certain email(s) and  
3 attachment(s) were potentially viewed by the hacker(s).<sup>5</sup> Therefore, during the Data  
4 Breach the hacker(s) were free to access, view, and exfiltrate Plaintiffs' and the  
5 Class's PII from Toshiba's email accounts, causing widespread damages to Plaintiffs  
6 and the Class.

7           4.     The PII accessed in the Data Breach included highly sensitive PII such  
8 as, names and Social Security numbers, (collectively, "Private Information").<sup>6</sup>

9           5.     Toshiba acquired, collected, and stored Plaintiffs' and Class Members'  
10 Private Information for employment purposes and through customer relationships.  
11 Therefore, at all relevant times, Toshiba knew or should have known that Plaintiffs'  
12 and Class Member's sensitive data, including their highly confidential PII, would be  
13 stored on Defendants' networks and email accounts.

14           6.     Toshiba could not perform its regular business activities or generate  
15 revenue without collecting and maintaining Plaintiffs' and Class Members' Private  
16 Information.

17           7.     Upon information and belief, Toshiba retains the Private Information it  
18 collects for many years, even after its relationships with Plaintiffs and Class  
19 Members ends.

20           8.     By obtaining, collecting, using, and deriving a benefit from Plaintiffs'  
21 and Class Members' PII, Toshiba assumed legal and equitable duties to Plaintiffs  
22 and the Class. Businesses that handle consumers' and employees' Private  
23 Information, like Toshiba, owe the individuals to whom the information relates a  
24 duty to adopt reasonable measures to protect it from disclosure to and theft by  
25

---

26 <sup>5</sup> *Id.*

27 <sup>6</sup> *Id.*

1 unauthorized third parties, and to keep it safe and confidential. This duty arises under  
2 contract, statutory and common law, industry standards, representations made to  
3 Plaintiffs and Class Members, and because it is foreseeable that hackers with  
4 nefarious intentions will target the Private Information and use it to harm the affected  
5 individuals.

6 9. Toshiba disregarded the rights of Plaintiffs and Class Members by  
7 intentionally, willfully, recklessly and/or negligently failing to take and implement  
8 adequate and reasonable measures to ensure that Plaintiffs' and Class Members' PII  
9 was safeguarded, failing to take available steps to prevent an unauthorized disclosure  
10 of data and failing to follow applicable, required and appropriate protocols, policies  
11 and procedures regarding the encryption of data, even for internal email use. As a  
12 result, the PII of Plaintiffs and Class Members was compromised through disclosure  
13 to a nefarious third-party that seeks to profit off this disclosure by defrauding  
14 Plaintiffs and Class Members in the future and by selling their information on the  
15 dark web.

16 10. The Data Breach, which Toshiba failed to detect until cybercriminals  
17 had already accessed, viewed, and stolen Plaintiffs' and Class Members' Private  
18 Information, is the direct result of Toshiba's failure to implement basic data security  
19 measures or oversight over Plaintiffs' and the Class's PII in its custody and control.  
20 Had Toshiba implemented reasonable cybersecurity measures—including adequate  
21 safeguards for initial access, encryption or redaction of personal data elements, and  
22 sufficient logging, monitoring, and alerting tools to detect unauthorized activity—  
23 criminals would not have been able to hack into Toshiba's email accounts, perform  
24 reconnaissance necessary to locate Plaintiffs' and Class Members' Private  
25 Information, and then access that data before being detected. The fact that Toshiba  
26 failed to detect the Breach for *months* is direct evidence of its negligence to  
27

1 implement industry standard data security measures.

2 11. Toshiba failed to adequately protect Plaintiffs' and Class Members'  
3 Private Information—and failed to even encrypt or redact this highly sensitive data  
4 when it was maintained on Toshiba's internet-accessible email accounts without  
5 adequate safeguards against unauthorized access and exfiltration. This unencrypted,  
6 unredacted Private Information was compromised due to Toshiba's negligent acts  
7 and omissions and utter failure to protect it.

8 12. Upon information and belief, the mechanism of the Data Breach and  
9 potential for improper disclosure of Plaintiffs' and Class Members' Private  
10 Information was a known risk to Toshiba, and thus, Toshiba knew that failing to take  
11 reasonable steps to secure the Private Information left it in a dangerous condition.

12 13. Due to Toshiba's negligent failure to secure and protect Plaintiffs' and  
13 Class Members' Private Information, cybercriminals accessed and obtained  
14 everything they need to commit identity theft and wreak havoc on the financial and  
15 personal lives of thousands of individuals.

16 14. Hackers targeted and obtained Plaintiffs' and Class Members' Private  
17 Information from Toshiba because of the data's value in exploiting and stealing  
18 Plaintiffs' and Class Members' identities. As a direct and proximate result of  
19 Toshiba's inadequate data security and breaches of its duties to handle Private  
20 Information with reasonable care, Plaintiffs' and Class Members' Private  
21 Information was accessed and acquired by cybercriminals and exposed to an untold  
22 number of unauthorized individuals. The present and continuing risk to Plaintiffs  
23 and Class Members as victims of the Data Breach will remain for their respective  
24 lifetimes.

25 15. The harm resulting from a data breach like this manifests in numerous  
26 ways including identity theft and financial fraud, and the exposure of an individual's  
27

1 Private Information due to breach ensures that the individual will be at a substantially  
2 increased and certainly impending risk of identity theft crimes compared to the rest  
3 of the population, potentially for the rest of his or her life. Mitigating that risk, to  
4 the extent even possible, requires individuals to devote significant time and money  
5 to closely monitor their credit, financial accounts, and email accounts, and take  
6 several additional prophylactic measures. Plaintiffs and Class Members will be  
7 forced to allocate time to these tasks for years, if not their lifetimes, due to Toshiba's  
8 Data Breach.

9 16. As a result of the Data Breach, Plaintiffs and Class Members suffered  
10 concrete injuries in fact including, but not limited to: (i) financial costs incurred  
11 mitigating the materialized risk and imminent threat of identity theft; (ii) loss of time  
12 and loss of productivity incurred mitigating the materialized risk and imminent  
13 threat of identity theft; (iii) actual identity theft and fraud; (iv) financial costs  
14 incurred due to actual identity theft; (v) loss of time incurred due to actual identity  
15 theft; (vi) deprivation of value of their Private Information; (vii) loss of privacy;  
16 (viii) emotional distress including anxiety and stress in with dealing with the Data  
17 Breach; and (ix) the continued risk to their sensitive Private Information, which  
18 remains in Toshiba's possession and subject to further data breaches, so long as  
19 Toshiba fails to undertake appropriate and adequate measures to protect the  
20 consumer data it collects and maintains.

21 17. Plaintiffs and Class Members have a continuing interest in ensuring that  
22 their Private Information is and remains safe, and they are entitled to injunctive and  
23 other equitable relief.

24 18. To recover for these harms, Plaintiffs, on behalf of themselves and the  
25 Class as defined herein, bring claims for negligence/negligence per se, breach of  
26 implied contract, unjust enrichment, and declaratory/injunctive relief, to address  
27

1 Toshiba's inadequate safeguarding of Plaintiffs' and Class Members' Private  
2 Information in its custody and Toshiba's failure to provide timely or adequate notice  
3 to Plaintiffs and Class Members that their information was compromised in the Data  
4 Breach.

5 19. Plaintiffs and Class Members seek compensatory, nominal, statutory,  
6 and punitive damages, declaratory judgment, and injunctive relief requiring Toshiba  
7 to: (i) disclose, expeditiously, the full nature of the Data Breach and the types of  
8 Private Information exposed; (ii) implement improved data security practices to  
9 reasonably guard against future breaches of Private Information in Toshiba's  
10 possession; and (iii) provide, at Toshiba's own expense, all impacted Data Breach  
11 victims with lifetime identity theft protection services.

## 12 II. THE PARTIES

13 20. **Plaintiff Kyle McDaniel** is an individual domiciled in Cordova,  
14 Tennessee. Plaintiff Kyle McDaniel received a Notice of Data Breach Letter from  
15 TGCS dated July 23, 2024, notifying him that his "*name and Social Security*  
16 *number were accessible to an unauthorized individual*" and compromised in the  
17 Data Breach.<sup>7</sup>

18 21. **Plaintiff Rikki McDaniel** is an individual domiciled in Cordova,  
19 Tennessee. Plaintiff Rikki McDaniel received a Notice of Data Breach Letter from  
20 TGCS dated November 26, 2024, notifying her that her "name and Social Security  
21 number were potentially accessible to an unauthorized individual" and compromised  
22 in the Data Breach.<sup>8</sup>

23 22. **Plaintiff Jon Williams** is an individual domiciled in Wilmington,  
24 North Carolina. Plaintiff Jon Williams received a Notice of Data Breach Letter from  
25

---

26 <sup>7</sup> Ex. 1 (Plaintiff Kyle McDaniel's Notice of Data Breach Letter) (emphasis added).

27 <sup>8</sup> Ex. 2 (Plaintiff Rikki McDaniel's Notice of Data Breach Letter).



1 TGCS dated July 23, 2024, notifying him that his “**name and Social Security**  
2 **number were accessible to an unauthorized individual**” and compromised in the  
3 Data Breach.<sup>9</sup>

4 23. **Plaintiff Mojdeh Williams** is an individual domiciled in Wilmington,  
5 North Carolina. Plaintiff Mojdeh Williams received a Notice of Data Breach Letter  
6 from TGCS dated November 26, 2024, notifying her that her “name and Social  
7 Security number were potentially accessible to an unauthorized individual” and  
8 compromised in the Data Breach.<sup>10</sup>

9 24. Defendant **Toshiba America Business Solutions, Inc. (“TABS”)**, is a  
10 corporation incorporated in California. Its principal place of business is located at  
11 25530 Commercentre Drive, Lake Forest, California 92630.

12 25. Defendant **Toshiba Global Commerce Solutions, Inc. (“TGCS”)** is a  
13 corporation incorporated in Delaware. Its principal place of business is located at  
14 3901 S. Miami Blvd., Durham, North Carolina 27703-9135.

15 **III. JURISDICTION AND VENUE**

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

22 27. Supplemental jurisdiction to adjudicate issues pertaining to state law is  
23 proper in this Court under 28 U.S.C. § 1367.

24 28. As previously stated, TABS is headquartered in this District and has its  
25

---

26 <sup>9</sup> Ex. 3 (Plaintiff Jon Williams’ Notice of Data Breach Letter) (Emphasis added).

27 <sup>10</sup> Ex. 4 (Plaintiff Mojdeh Williams’ Notice of Data Breach Letter).



principal place of business in this District. Defendants also have sufficient minimum contacts in California and have intentionally availed themselves to this jurisdiction by marketing and selling products and services and by accepting and processing payments for those products and services within California.

29. Venue is proper in this Court under 28 U.S.C. § 1391(b)(1) because a substantial part of the events that gave rise to Plaintiffs' claims took place within this District, including the Data Breach at issue.

#### IV. FACTUAL ALLEGATIONS

##### A. Toshiba Collects and Stores Plaintiffs' and the Class's PII.

20. TABS is a subsidiary of Toshiba TEC Corporation and provides office printing and retail solutions.<sup>11</sup> TABS has offices across the U.S. and Latin America, and a production facility in Mitchell, South Dakota that manufactures toner for the U.S. and global markets.<sup>12</sup>

21. TGCS is a global market share leader in retail store technology.<sup>13</sup> There are over 2,000 employees working for TGCS serving over 120 countries worldwide.<sup>14</sup>

22. According to Toshiba's latest financial reports the company's current revenue (TTM ) is \$23.53 Billion USD.<sup>15</sup>

---

<sup>11</sup> *Contact Us*, TOSHIBA, <https://business.toshiba.com/about/contact-us> (last visited Dec. 10, 2024).

<sup>12</sup> *Id.*

<sup>13</sup> TOSHIBA, <https://commerce.toshiba.com/wps/portal/marketing/?urile=wcm:path:/en-us/home> (last visited Dec. 10, 2024).

<sup>14</sup> *About Us*, TOSHIBA, <https://commerce.toshiba.com/wps/portal/marketing/?urile=wcm:path:/en-us/home/company/about-us> (last visited Dec. 10, 2024).

<sup>15</sup> *Toshiba*, COMPANIES MARKET CAP, [https://companiesmarketcap.com/toshiba/revenue/#:~:text=Revenue%20in%202023%20\(TTM\)%3A,were%20of%20%2429.58%20Billion%20USD](https://companiesmarketcap.com/toshiba/revenue/#:~:text=Revenue%20in%202023%20(TTM)%3A,were%20of%20%2429.58%20Billion%20USD) (last visited Dec. 10, 2024).

1           23. Toshiba could have afforded to implement adequate data security prior  
2 to the Data Breach but deliberately chose not to.

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

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

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

13           27. Both Defendants recognize this duty and make the following claims on  
14 their websites regarding their protection of sensitive data:

15  
16           **TGCS:**

17           Toshiba has implemented technical and organizational  
18 security measures to guarantee the security of your  
19 Personal Information. Users' Personal Information is  
20 stored in our secure networks and access is restricted to  
21 those employees and partners who are entitled to access  
22 our systems.<sup>16</sup>

23           **TABS:**

24           Toshiba has implemented technical and organizational  
25 security measures to provide reasonable security for your

---

26 <sup>16</sup> *Privacy Policy*, TOSHIBA, [https://commerce.toshiba.com/?urile=wcm:path:/en-us/common-content/general-content/privacy-](https://commerce.toshiba.com/?urile=wcm:path:/en-us/common-content/general-content/privacy-policy&mapping=tgcs_new.portal.generalDetails)  
27 [policy&mapping=tgcs\\_new.portal.generalDetails](https://commerce.toshiba.com/?urile=wcm:path:/en-us/common-content/general-content/privacy-policy&mapping=tgcs_new.portal.generalDetails) (last visited Dec. 10, 2024).

1 Personal Information. Users' Personal Information is  
2 stored in our secure networks and access is restricted to  
3 those employees and partners who are entitled to access  
4 our systems.<sup>17</sup>

5 28. Toshiba's assurances of maintaining high standards of cybersecurity  
6 make it evident that Toshiba recognized it had a duty to use reasonable measures to  
7 protect the PII that it collected and maintained.

8 29. Toshiba violated its own Privacy Policies and failed to adopt reasonable  
9 and appropriate security practices and procedures including administrative, physical  
10 security, and technical controls to safeguard Plaintiffs' and the Class's Private  
11 Information.

12 30. At all relevant times, Toshiba knew it was storing and using its email  
13 accounts to store and transmit valuable, sensitive Private Information and that as a  
14 result, its email accounts would be attractive targets for cybercriminals.

15 31. Toshiba also knew that any breach of its email accounts and exposure  
16 of the data stored therein would result in the increased risk of identity theft and fraud  
17 for the thousands of individuals whose Private Information was compromised, as  
18 well as intrusion into their private and sensitive personal matters.

19 32. Despite knowledge of their duties to keep Plaintiffs' and Class  
20 Members' PII secure, Toshiba failed to adequately protect its email accounts from  
21 unauthorized access. As a result, Plaintiffs' and Class Members' PII was accessed  
22 and stolen from Toshiba's inadequately secured email systems in a massive and  
23 preventable Data Breach.

24 **B. Toshiba's Massive and Preventable Data Breach.**

25 33. On an undisclosed date, Toshiba discovered suspicious activity within  
26

---

27 <sup>17</sup> *Privacy Policy*, TOSHIBA, <https://business.toshiba.com/privacy-policy> (last visited  
28 Dec. 10, 2024).

1 its email environment.<sup>18</sup>

2 34. After detecting the Breach, Toshiba claims it initiated an investigation  
3 in which it determined cybercriminals infiltrated Toshiba's email environment  
4 between December 4, 2023, and March 18, 2024.<sup>19</sup>

5 35. Toshiba gives no explanation why the Data Breach was allowed to  
6 continue for over three (3) months or why Toshiba failed to detect the Breach until  
7 months after it initially began.

8 36. Toshiba claims the investigation of the Data Breach is still ongoing, but  
9 on May 14, 2024, it learned that personal information was potentially viewed by an  
10 unauthorized individual.<sup>20</sup>

11 37. The Private Information accessed without authorization in the Data  
12 Breach included highly sensitive information such as Social Security numbers and  
13 names—which can immediately be used to commit fraud and identity theft.<sup>21</sup>

14 38. Despite the Data Breach beginning in December 2023, Toshiba did not  
15 begin notifying individuals of the Data Breach until May 28, 2024,<sup>22</sup> with some not  
16 being notified until July 2024 or November 2024.<sup>23</sup>

17 39. Omitted from the Notice of Data Breach Letters were the details of the  
18 root cause of the Data Breach, the vulnerabilities exploited, when the Data Breach

---

19 <sup>18</sup> OFFICE OF THE MAINE ATTORNEY GENERAL, *Toshiba America Business Solutions*,  
20 [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)  
21 [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) (last visited Dec. 7,  
22 2024); OFFICE OF THE MAINE ATTORNEY GENERAL, *Toshiba Global Commerce*  
23 *Solutions*, [https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8fea1aeb-d918-4c0d-b40d-97990f1eb395.html)  
24 [a1252b4f8318/8fea1aeb-d918-4c0d-b40d-97990f1eb395.html](https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8fea1aeb-d918-4c0d-b40d-97990f1eb395.html) (last visited Dec. 7,  
25 2024).

24 <sup>19</sup> *Id.*

25 <sup>20</sup> *Id.*

26 <sup>21</sup> *Id.*

27 <sup>22</sup> *Id.*

28 <sup>23</sup> *See* Exs. 1–4.

1 began and ended, and the remedial measures undertaken to ensure such a breach  
2 does not occur again. To date, these critical facts have not been explained or clarified  
3 to Plaintiffs and Class Members, who retain a vested interest in ensuring that their  
4 Private Information is protected.

5 40. Toshiba's purported disclosure amounts to no real disclosure at all, as  
6 it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts,  
7 like the status of Toshiba's investigation or the nature of Private Information  
8 involved, with any degree of specificity or uniformity. Without these details,  
9 Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data  
10 Breach is severely diminished.

11 41. Plaintiffs' and Class Members' Private Information was targeted,  
12 accessed, and stolen by cybercriminals in the Data Breach. Toshiba's insufficient  
13 security for Plaintiffs' and the Class's PII caused and allowed criminals to target and  
14 take files containing Plaintiffs' and Class Members' inadequately protected,  
15 unencrypted Private Information from Toshiba's email accounts, and unreasonably  
16 delayed Plaintiffs' and Class Members' notice by months.

17 42. As the Data Breach and its timeline evidences, Toshiba did not use  
18 reasonable security measures appropriate to the nature of the sensitive Private  
19 Information collected from Plaintiffs and Class Members and maintained on  
20 Toshiba's emails, such as encrypting the information, deleting the data from  
21 Toshiba's emails accounts when it was no longer needed, requiring sufficient  
22 verification such as multi-factor authentication for email accounts, training  
23 employees about cybersecurity, phishing, and attempts to gain unauthorized access,  
24 investigating and addressing vulnerabilities in its data security practices, and/or  
25 implementing the necessary safeguards to enable Toshiba to identify malicious  
26 activity and curtail it when it happens. These failures allowed and caused  
27

1 cybercriminals to target Toshiba's email accounts and carry out the Data Breach.

2 43. Toshiba could and should have prevented this Data Breach by ensuring  
3 its email accounts containing Plaintiffs' and Class Members' Private Information  
4 were properly secured, sanitized, and encrypted and by using appropriate  
5 clearinghouse practices to purge consumer data that it was no longer required to  
6 maintain, but failed to do so.

7 44. Toshiba could and should have properly monitored its email accounts  
8 for unauthorized access and unusual activity, including the downloading of large  
9 amounts of sensitive personal information from its email accounts.

10 45. Additionally, Toshiba could have prevented this Data Breach by  
11 examining, testing, and updating its cybersecurity practices to ensure vulnerabilities  
12 were identified and addressed and reasonable safeguards were continuously  
13 maintained, but failed to do so.

14 46. In recognition of the severity of the Data Breach, and the imminent risk  
15 of harm Plaintiffs and the Class face, Toshiba made an offering of twenty-four (24)  
16 months of identity theft protection services.<sup>24</sup> Such an offering is inadequate and will  
17 not prevent identity theft but will only alert Data Breach victims once identity theft  
18 has *already occurred*.

19 47. All in all, Toshiba failed to take the necessary precautions required to  
20 safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access  
21 and exploitation.

22 48. Defendants' actions represent a flagrant disregard of the rights of  
23 Plaintiffs and the Class, both as to privacy and property.

24 **C. Cyber Criminals Have Used and Will Continue to Use Plaintiffs' and the**  
25 **Class's PII to Defraud Them.**

---

26  
27 <sup>24</sup> *Id.*

1           49. PII is of great value to hackers and cybercriminals, and the data stolen  
2 in the Data Breach can and will be used in a variety of ways by criminals to exploit  
3 Plaintiffs and the Class Members and to profit off their misfortune.

4           50. Each year, identity theft causes tens of billions of dollars of losses to  
5 victims in the United States.<sup>25</sup>

6           51. For example, with the PII stolen in the Data Breach, including Social  
7 Security numbers, identity thieves can open financial accounts, apply for credit, file  
8 fraudulent tax returns, commit crimes, create false driver's licenses and other forms  
9 of identification and sell them to other criminals or undocumented immigrants, steal  
10 government benefits, give breach victims' names to police during arrests, and many  
11 other harmful forms of identity theft.<sup>26</sup> These criminal activities have and will result  
12 in devastating financial and personal losses to Plaintiffs and the Class Members.

13           52. Social security numbers are particularly sensitive pieces of personal  
14 information. As the Consumer Federation of America explains:

15  
16           **Social Security number.** *This is the most dangerous type of personal*  
17 *information in the hands of identity thieves* because it can open the gate  
18 to serious fraud, from obtaining credit in your name to impersonating  
19 you to get medical services, government benefits, your tax refunds,  
20 employment – even using your identity in bankruptcy and other legal  
21  
22

---

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

26 <sup>26</sup> *See, e.g.,* Christine DiGangi, *What Can You Do with a Stolen Social Security*  
27 *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/>.



1 matters. It's hard to change your Social Security number and it's not a  
2 good idea because it is connected to your life in so many ways.<sup>27</sup>  
3 (Emphasis added).

4 53. PII is such a valuable commodity to identity thieves that once it has  
5 been compromised, criminals will use it for years.<sup>28</sup>

6 54. This was a financially motivated breach, as the only reason the  
7 cybercriminals go through the trouble of running targeted cyberattacks against  
8 companies like Toshiba is to get ransom money and/or information that they can  
9 monetize by selling on the black market for use in the kinds of criminal activity  
10 described herein.

11 55. Indeed, a social security number, date of birth, and full name can sell  
12 for \$60 to \$80 on the digital black market.<sup>29</sup>

13 56. "[I]f there is reason to believe that your personal information has been  
14 stolen, you should assume that it can end up for sale on the dark web."<sup>30</sup>  
15  
16  
17  
18

---

19 <sup>27</sup> *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF  
20 AMERICA (Mar. 19, 2019), [https://consumerfed.org/consumer\\_info/dark-web-](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/)  
21 [monitoring-what-you-should-know/](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/).

22 <sup>28</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;*  
23 *However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at  
<https://www.gao.gov/products/gao-07-737>.

24 <sup>29</sup> Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web* (Nov.  
25 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)  
[on-the-dark-web](https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web).

26 <sup>30</sup> *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/)  
[monitoring-what-you-should-know/](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/).

1           57. These risks are both certainly impending and substantial. As the Federal  
2 Trade Commission (“FTC”) has reported, if hackers get access to PII, ***they will use***  
3 ***it***.<sup>31</sup>

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

7           [I]n some cases, stolen data may be held for up to a year or more before  
8 being used to commit identity theft. Further, once stolen data have been  
9 sold or posted on the Web, fraudulent use of that information ***may***  
10 ***continue for years***. As a result, studies that attempt to measure the harm  
11 resulting from data breaches cannot necessarily rule out all future  
harm.<sup>32</sup>

12           59. For instance, with a stolen Social Security number, which is part of the  
13 PII compromised in the Data Breach, a criminal can (i) obtain credit cards or loans;  
14 (ii) open a new bank account; (iii) empty existing bank accounts; (iv) get a fraudulent  
15 driver’s license; (v) receive medical care; (vi) open a phone account; (vii) commit  
16 crimes that will show up on the victim’s record; (viii) steal benefits and Social  
17 Security checks; (ix) set up utilities; and file a fraudulent tax returns.<sup>33</sup>

18           60. Identity thieves have already started to prey on the Toshiba Data Breach  
19 victims, and we can anticipate that this will continue.  
20  
21

---

22 <sup>31</sup> Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER  
23 (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)  
24 [thieves-use-stolen-info](https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info).

25 <sup>32</sup> *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited;*  
26 *However, the Full Extent Is Unknown*, GAO (July 5, 2007), available at  
27 <https://www.gao.gov/products/gao-07-737>.

<sup>33</sup> [https://www.aura.com/learn/what-can-someone-do-with-your-social-security-](https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number)  
number.

1           61. Identity theft victims must spend countless hours and large amounts of  
2 money repairing the impact to their credit as well as protecting themselves in the  
3 future.<sup>34</sup>

4           62. Defendants' offer of two (2) years of identity monitoring to Plaintiffs  
5 and the Class is woefully inadequate and will not fully protect Plaintiffs from the  
6 damages and harm caused by its failures.

7           63. The full scope of the harm has yet to be realized. There may be a time  
8 lag between when harm occurs versus when it is discovered, and between when PII  
9 is stolen and when it is used.

10           64. Once the twenty-four months have expired, Plaintiffs and Class  
11 Members will need to pay for their own identity theft protection and credit  
12 monitoring for the rest of their lives due to Toshiba's gross negligence.

13           65. Furthermore, identity monitoring only alerts someone to the fact that  
14 they have *already been the victim of identity theft* (i.e., fraudulent acquisition and  
15 use of another person's PII)—it does not prevent identity theft.<sup>35</sup> Nor can an identity  
16 monitoring service remove personal information from the dark web.<sup>36</sup>

17           66. "The people who trade in stolen personal information [on the dark web]  
18 won't cooperate with an identity theft service or anyone else, so it's impossible to  
19  
20

---

21  
22 <sup>34</sup> *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept.  
23 2013), available at [https://www.global-screeningsolutions.com/Guide-for-](https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf)  
24 [Assisting-ID-Theft-Victims.pdf](https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf).

25 <sup>35</sup> See, e.g., Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*,  
26 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)  
27 [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).

28 <sup>36</sup> *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF  
AMERICA (Mar. 19, 2019), [https://consumerfed.org/consumer\\_info/dark-web-](https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know)  
monitoring-what-you-should-know.

1 get the information removed, stop its sale, or prevent someone who buys it from  
2 using it.”<sup>37</sup>

3 67. As a direct and proximate result of the Data Breach, Plaintiffs and the  
4 Class have been damaged and have been placed at an imminent, immediate, and  
5 continuing increased risk of harm from continued fraud and identity theft. Plaintiffs  
6 and the Class must now take the time and effort to mitigate the actual and potential  
7 impact of the Data Breach on their everyday lives, including placing “freezes” and  
8 “alerts” with credit reporting agencies, contacting their financial institutions, closing  
9 or modifying financial accounts, and closely reviewing and monitoring bank  
10 accounts and credit reports for unauthorized activity for years to come.

11 68. Even more seriously is the identity restoration that Plaintiffs and other  
12 Class Members must go through, which can include spending countless hours filing  
13 police reports, filling out IRS forms, Federal Trade Commission checklists,  
14 Department of Motor Vehicle driver’s license replacement applications, and calling  
15 financial institutions to cancel fraudulent credit applications, to name just a few of  
16 the steps Plaintiffs and the Class must take.

17 69. Plaintiffs and the Class have or will experience the following concrete  
18 and particularized harms for which they are entitled to compensation, including:

- 19 a. Actual identity theft;
- 20 b. Trespass, damage to, and theft of their personal property including PII;
- 21 c. Improper disclosure of their PII;
- 22 d. The imminent and certainly impending injury flowing from potential  
23 fraud and identity theft posed by their PII being placed in the hands of  
24 criminals;
- 25 e. Loss of privacy suffered as a result of the Data Breach, including the

---

26  
27 <sup>37</sup> *Id.*

1 harm of knowing cybercriminals have their PII;

2 f. Ascertainable losses in the form of time taken to respond to identity  
3 theft and attempt to restore identity, including lost opportunities and  
4 lost wages from uncompensated time off from work;

5 g. Ascertainable losses in the form of out-of-pocket expenses and the  
6 value of their time reasonably expended to remedy or mitigate the  
7 effects of the Data Breach;

8 h. Ascertainable losses in the form of deprivation of the value of  
9 Plaintiffs' and Class Members' Private Information for which there is  
10 a well-established and quantifiable national and international market;

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

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

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

15 70. Moreover, Plaintiffs and Class Members have an interest in ensuring  
16 that their Private Information, which remains in the possession of Defendants, is  
17 protected from further breaches by the implementation of industry standard security  
18 measures and safeguards. Defendants have shown themselves wholly incapable of  
19 protecting Plaintiffs' and the Class's Private Information.

20 71. Plaintiffs and Class Members also have an interest in ensuring that their  
21 Private Information that was provided to Toshiba is removed from all of Toshiba's  
22 servers, email systems, and files.

23 72. Defendants themselves acknowledged the harm caused by the Data  
24 Breach because they offered Plaintiffs and Class Members woefully inadequate  
25 identity theft repair and monitoring services. Twenty-four (24) months of identity  
26  
27  
28

1 theft and repair and monitoring is, however, inadequate to protect Plaintiffs and  
2 Class Members from a lifetime of identity theft risk.

3 73. Defendants further acknowledged that the Data Breach would cause  
4 inconvenience to affected individuals and that financial harm would likely occur,  
5 stating, “[w]e regret any inconvenience or concern this incident may have caused  
6 you.”<sup>38</sup>

7 74. Additionally, the Notice of Data Breach Letter sent to Plaintiffs and  
8 other Class Members recognized that Toshiba needed to improve its cybersecurity  
9 protocols, stating “[t]o help prevent a similar incident from occurring in the future,  
10 we implemented additional measures to enhance the security of our email  
11 environment.”<sup>39</sup>

12 75. These enhanced protections should have been in place before the Data  
13 Breach.

14 76. At Toshiba’s suggestion, Plaintiffs are desperately trying to mitigate  
15 the damage that Toshiba has caused them.

16 77. Given the kind of Private Information Toshiba made accessible to  
17 hackers, however, Plaintiffs are certain to incur additional damages. Because  
18 identity thieves have their PII, Plaintiffs and all Class Members will need to have  
19 identity theft monitoring protection for the rest of their lives. Some may even need  
20 to go through the long and arduous process of getting a new Social Security number,  
21 with all the loss of credit and employment difficulties that come with a new  
22 number.<sup>40</sup>

---

23  
24 <sup>38</sup> Ex. 2.

25 <sup>39</sup> *Id.*

26 <sup>40</sup> *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10,  
27 2022), <https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html>.

1 78. None of this should have happened because the Data Breach was  
2 entirely preventable.

3 **D. Defendants were Aware of the Risk of Cyberattacks.**

4 79. Toshiba's negligence, including its gross negligence, in failing to  
5 safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the  
6 repeated warnings and alerts directed to protecting and securing sensitive data.

7 80. Private Information of the kind accessed in the Data Breach is of great  
8 value to cybercriminals as it can be used for a variety of unlawful and nefarious  
9 purposes, fraudulent misuse and sale on the internet black market known as the dark  
10 web.

11 81. Private Information can also be used to distinguish, identify, or trace an  
12 individual's identity, such as his or her name, Social Security number, and financial  
13 records. This may be accomplished alone, or in combination with other personal or  
14 identifying information connected or linked to an individual such as his or her  
15 birthdate, birthplace, and mother's maiden name.

16 82. Data thieves regularly target entities that store Private Information like  
17 Toshiba due to the highly sensitive information they maintain. Toshiba knew and  
18 understood that Plaintiffs' and Class Members' Private Information is valuable and  
19 highly sought after by criminal parties who seek to illegally monetize it through  
20 unauthorized access.

21 83. Cyberattacks against institutions such as Toshiba are targeted and  
22 frequent. According to the Identity Theft Resource Center's report covering the year  
23 2021, "the overall number of data compromises (1,862) is up more than 68 percent  
24 compared to 2020. The new record number of data compromises is 23 percent over  
25 the previous all-time high (1,506) set in 2017. The number of data events that  
26 involved sensitive information (Ex: Social Security numbers) increased slightly  
27



1 compared to 2020 (83 percent vs. 80 percent).” As stated in IBM’s 2022 report,  
2 “[f]or 83% of companies, it’s not if a data breach will happen, but when.”

3 84. The increase in such attacks, and attendant risk of future attacks, was  
4 widely known to the public and to anyone in Toshiba’s industry, including Toshiba  
5 itself.

6 85. Toshiba’s data security obligations were particularly important given  
7 the substantial increase preceding the date of the subject Data Breach, in  
8 cyberattacks and/or data breaches targeting entities like Toshiba that collect and  
9 store PII.

10 86. In 2023, an all-time high for data compromises occurred, with 3,205  
11 compromises affecting 353,027,892 total victims. The estimated number of  
12 organizations impacted by data compromises has increased by +2,600 percentage  
13 points since 2018, and the estimated number of victims has increased by +1400  
14 percentage points. The 2023 compromises represent a 78-percentage point increase  
15 over the previous year and a 72-percentage point hike from the previous all-time  
16 high number of compromises (1,862) set in 2021.

17 87. Additionally, as companies became more dependent on computer  
18 systems to run their business, e.g., working remotely as a result of the Covid-19  
19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is  
20 magnified, thereby highlighting the need for adequate administrative, physical, and  
21 technical safeguards.

22 88. Businesses operating in the technology sector, such as Toshiba, are a  
23 “wealth of sensitive data,” and are “prime targets for hackers seeking financial gain,  
24 intellectual property theft, or simply to wreak havoc.”<sup>41</sup>

25 89. Toshiba knew or should have known of the inherent risks in collecting  
26

---

27 <sup>41</sup> <https://www.offsec.com/blog/top-technology-sector-breaches-and-threats/>.

1 and storing Private Information and the critical importance of providing adequate  
2 security for it.

3 90. Toshiba was clearly aware of the risks it was taking and the harm that  
4 could result from inadequate data security but threw caution to the wind.

5 91. As a business in possession of customers' Private Information, Toshiba  
6 knew, or should have known, the importance of safeguarding the Private Information  
7 entrusted to it, directly and indirectly, by Plaintiffs and Class Members, and of the  
8 foreseeable consequences if its network systems were breached. Such consequences  
9 include the significant costs imposed on Plaintiffs and Class Members due to their  
10 Private Information's disclosure to cybercriminals. Nevertheless, Toshiba failed to  
11 implement or follow reasonable cybersecurity measures to protect against the  
12 foreseeable harm of this Data Breach.

13 92. Given the nature of the Data Breach, it was foreseeable that Plaintiffs'  
14 and Class Members' Private Information compromised therein would be targeted by  
15 hackers and cybercriminals for use in variety of different injurious ways. Indeed,  
16 the cybercriminals who possess Plaintiffs' and Class Members' Private Information  
17 can easily obtain their tax returns or open fraudulent credit card accounts in  
18 Plaintiffs' and Class Members' names.

19 93. Plaintiffs and Class Members were the foreseeable and probable  
20 victims of Toshiba's inadequate security practices and procedures. The breadth of  
21 data compromised in the Data Breach makes the information particularly valuable  
22 to thieves and leaves Plaintiffs and Class Members especially vulnerable to identity  
23 theft, medical and financial fraud, and the like.

**E. Toshiba Could Have Prevented the Data Breach.**

94. Data breaches are preventable.<sup>42</sup> 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.”<sup>43</sup> 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 . . . .”<sup>44</sup>

95. “Most of the 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*.”<sup>45</sup>

96. In a data breach like this, many failures laid the groundwork for the Breach.

97. The FTC has published guidelines that establish reasonable data security practices for businesses.

98. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.<sup>46</sup>

---

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

<sup>43</sup>*Id.* at 17.

<sup>44</sup>*Id.* at 28.

<sup>45</sup>*Id.*

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

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

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

10           101. According to information and belief, Toshiba failed to maintain many  
11 reasonable and necessary industry standards necessary to prevent a data breach,  
12 including the FTC's guidelines.

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

19           103. As explained by the Federal Bureau of Investigation, "[p]revention is  
20 the most effective defense against ransomware and it is critical to take precautions  
21 for protection."<sup>47</sup>

---

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

1           104. To prevent and detect malware attacks, including the malware attack  
2 that resulted in the Data Breach, Defendants could and should have implemented, as  
3 recommended by the Federal Bureau of Investigation, the following measures:

- 4           • Implement an awareness and training program. Because end users  
5 are targets, employees and individuals should be aware of the threat  
6 of ransomware and how it is delivered.
- 7           • Enable strong spam filters to prevent phishing emails from reaching  
8 the end users and authenticate inbound email using technologies like  
9 Sender Policy Framework (SPF), Domain Message Authentication  
10 Reporting and Conformance (DMARC), and DomainKeys  
11 Identified Mail (DKIM) to prevent email spoofing.
- 12          • Scan all incoming and outgoing emails to detect threats and filter  
13 executable files from reaching end users.
- 14          • Configure firewalls to block access to known malicious IP  
15 addresses.
- 16          • Patch operating systems, software, and firmware on devices.  
17 Consider using a centralized patch management system.
- 18          • Set anti-virus and anti-malware programs to conduct regular scans  
19 automatically.
- 20          • Manage the use of privileged accounts based on the principle of least  
21 privilege: no users should be assigned administrative access unless  
22 absolutely needed; and those with a need for administrator accounts  
23 should only use them when necessary.
- 24          • Configure access controls—including file, directory, and network  
25 share permissions—with least privilege in mind. If a user only needs  
26 to read specific files, the user should not have write access to those  
27

1 files, directories, or shares.

- 2 • Disable macro scripts from office files transmitted via email.
- 3 Consider using Office Viewer software to open Microsoft Office
- 4 files transmitted via email instead of full office suite applications.
- 5 • Implement Software Restriction Policies (SRP) or other controls to
- 6 prevent programs from executing from common ransomware
- 7 locations, such as temporary folders supporting popular Internet
- 8 browsers or compression/decompression programs, including the
- 9 AppData/LocalAppData folder.
- 10 • Consider disabling Remote Desktop protocol (RDP) if it is not being
- 11 used.
- 12 • Use application whitelisting, which only allows systems to execute
- 13 programs known and permitted by security policy.
- 14 • Execute operating system environments or specific programs in a
- 15 virtualized environment.
- 16 • Categorize data based on organizational value and implement
- 17 physical and logical separation of networks and data for different
- 18 organizational units.<sup>48</sup>

19 105. Further, to prevent and detect malware attacks, Defendants could and  
20 should have implemented, as recommended by the United States Cybersecurity &  
21 Infrastructure Security Agency, the following measures:

- 22 • **Update and patch your computer.** Ensure your applications and
- 23 operating systems (OSs) have been updated with the latest patches.
- 24 Vulnerable applications and OSs are the target of most ransomware
- 25 attacks....

---

26 <sup>48</sup> *Id.* at 3–4.

27

- 1       • **Use caution with links and when entering website addresses.** Be  
2       careful when clicking directly on links in emails, even if the sender  
3       appears to be someone you know. Attempt to independently verify  
4       website addresses (e.g., contact your organization's helpdesk, search  
5       the internet for the sender organization's website or the topic  
6       mentioned in the email). Pay attention to the website addresses you  
7       click on, as well as those you enter yourself. Malicious website  
8       addresses often appear almost identical to legitimate sites, often  
9       using a slight variation in spelling or a different domain (e.g., .com  
10      instead of .net)....
- 11      • **Open email attachments with caution.** Be wary of opening email  
12      attachments, even from senders you think you know, particularly  
13      when attachments are compressed files or ZIP files.
- 14      • **Keep your personal information safe.** Check a website's security  
15      to ensure the information you submit is encrypted before you  
16      provide it....
- 17      • **Verify email senders.** If you are unsure whether or not an email is  
18      legitimate, try to verify the email's legitimacy by contacting the  
19      sender directly. Do not click on any links in the email. If possible,  
20      use a previous (legitimate) email to ensure the contact information  
21      you have for the sender is authentic before you contact them.
- 22      • **Inform yourself.** Keep yourself informed about recent  
23      cybersecurity threats and up to date on ransomware techniques. You  
24      can find information about known phishing attacks on the Anti-  
25      Phishing Working Group website. You may also want to sign up for  
26      CISA product notifications, which will alert you when a new Alert,  
27



1 Analysis Report, Bulletin, Current Activity, or Tip has been  
2 published.

- 3 • **Use and maintain preventative software programs.** Install  
4 antivirus software, firewalls, and email filters—and keep them  
5 updated—to reduce malicious network traffic....<sup>49</sup>

6 106. In addition, to prevent and detect ransomware attacks, including the  
7 ransomware attack that resulted in the Data Breach, Defendants could and should  
8 have implemented, as recommended by the Microsoft Threat Protection Intelligence  
9 Team, the following measures:

- 10 • **Secure internet-facing assets**
  - 11 - Apply latest security updates
  - 12 - Use threat and vulnerability management
  - 13 - Perform regular audit; remove privileged credentials
- 14 • **Thoroughly investigate and remediate alerts**
  - 15 - Prioritize and treat commodity malware infections as
  - 16 potential full compromise;
- 17 • **Include IT Pros in security discussions**
  - 18 - Ensure collaboration among [security operations],
  - 19 [security admins], and [information technology] admins to
  - 20 configure servers and other endpoints securely;
- 21 • **Build credential hygiene**

22  
23  
24  
25 <sup>49</sup> 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).

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

- **Apply principle of least-privilege**

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

- **Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>50</sup>

107. Moreover, the FTC has promulgated materials centered on how to prevent phishing attacks and recommends businesses take the following actions:

- **Back Up Your Data:** Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

---

<sup>50</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), available at <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/>.

- 1       • **Keep Your Security Up to Date:** Always install the latest patches  
2       and updates. Look for additional means of protection, like email  
3       authentication and intrusion prevention software, and set them to  
4       update automatically on your computers. On mobile devices, you  
5       may have to do it manually.
- 6       • **Alert Your Staff:** Share with them this information. Keep in mind  
7       that phishing scammers change their tactics often, so make sure you  
8       include tips for spotting the latest phishing schemes in your regular  
9       training.
- 10      • **Deploy a Safety Net:** Use email authentication technology to help  
11      prevent phishing emails from reaching your company's inboxes in  
12      the first place.<sup>51</sup>

13       108. Upon information and belief, Toshiba failed to take any of the industry  
14      standard precautions above, culminating in the Data Breach.

15       109. Given that Defendants were storing the PII of thousands of  
16      individuals, Defendants could have and should have implemented all the above  
17      measures to prevent and detect cyber intrusions.

18       110. Specifically, among other failures, Toshiba had far too much  
19      confidential unencrypted information held on its email systems. Such PII should  
20      have been segregated into an encrypted system.<sup>52</sup>

21       111. Moreover, it is well-established industry standard practice for a  
22      business to dispose of confidential PII once it is no longer needed.

---

24      <sup>51</sup>[https://www.ftc.gov/system/files/attachments/phishing/cybersecurity\\_sb\\_phishing.pdf](https://www.ftc.gov/system/files/attachments/phishing/cybersecurity_sb_phishing.pdf).

25      <sup>52</sup> See, e.g., Adnan Raja, *How to Safeguard Your Business Data with Encryption*,  
26      FORTRA (Aug. 14, 2018), <https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption>.  
27

1 112. The FTC, among others, has repeatedly emphasized the importance of  
2 disposing unnecessary PII, saying simply: “Keep sensitive data in your system only  
3 as long as you have a business reason to have it. Once that business need is over,  
4 properly dispose of it. If it’s not on your system, it can’t be stolen by hackers.”<sup>53</sup>  
5 Toshiba, rather than following this basic standard of care, kept thousands of  
6 individuals’ unencrypted PII indefinitely.

7 113. In sum, the Data Breach could have readily been prevented through the  
8 use of industry standard network segmentation and encryption of all PII.

9 114. Further, the scope of the Data Breach could have been dramatically  
10 reduced had Toshiba utilized proper record retention and destruction practices.

#### 11 **F. Plaintiffs’ Individual Experiences**

##### 12 ***Plaintiff Kyle McDaniel***

13 115. Plaintiff Kyle McDaniel received a Notice of Data Breach Letter from  
14 TGCS informing him that his highly confidential Private Information was  
15 compromised in the Data Breach.

16 116. Plaintiff Kyle McDaniel is a former employee of Toshiba.

17 117. Defendants were in possession of Plaintiff Kyle McDaniel’s Private  
18 Information before, during, and after the Data Breach.

19 118. Because of the Data Breach, there is no doubt Plaintiff Kyle  
20 McDaniel’s highly confidential Private Information is in the hands of  
21 cybercriminals. Reason being, the Notice of Data Breach Letter from TGCS  
22 disclosed that an unauthorized third-party accessed Defendants’ system. The *modus*  
23 *operandi* of cybercriminals involves stealing Private Information for financial gain.

---

24  
25 <sup>53</sup> *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), at p. 6.

1 Cybercriminals may use stolen identities to conceal their own true identity or carry  
2 out a range of fraudulent activities, from credit card fraud to impersonation. As such,  
3 Plaintiff Kyle McDaniel and the Class are at imminent risk of identity theft and  
4 fraud.

5 119. As a result of the Data Breach, Plaintiff Kyle McDaniel has already  
6 expended over **100 hours** of his time and has suffered loss of productivity from  
7 taking time to address and attempt to ameliorate, mitigate, and address the future  
8 consequences of the Data Breach. This includes: (i) investigating the Data Breach;  
9 (ii) investigating how best to ensure that he is protected from identity theft; (iii)  
10 reviewing his account statements, credit reports, and/or other information; and (iv)  
11 mitigating the fraud and identity theft he has already experienced.

12 120. Plaintiff Kyle McDaniel has already suffered misuse of his Private  
13 Information because of the Data Breach. On June 9, 2024, Plaintiff Kyle McDaniel  
14 received a letter from Chase Bank informing him that someone was fraudulently  
15 using his personal information and attempted to open a financial account in his name.  
16 In response, Plaintiff Kyle McDaniel placed a fraud alert on his credit with Experian,  
17 Equifax, and TransUnion and froze his credit. Plaintiff Kyle McDaniel estimates he  
18 has spent at least 24 hours remedying the fraud he experienced alone. This instance  
19 of fraud is not a coincidence. The PII exposed in the Breach are precisely the types  
20 of PII needed to perpetrate this type of fraud.

21 121. Due to the fraud and identity theft Plaintiff experienced from the Data  
22 Breach, Plaintiff was forced to purchase Bit Defender Total Security.

23 122. Plaintiff Kyle McDaniel places significant value in the security of his  
24 Private Information and does not readily disclose it. Plaintiff Kyle McDaniel has  
25 never knowingly transmitted unencrypted Private Information over the internet or  
26 any other unsecured source.

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

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

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

19           126. Plaintiff Kyle McDaniel has suffered injuries directly and proximately  
20 caused by the Data Breach, including: (i) theft of his valuable Private Information;  
21 (ii) the imminent and certain impending injury flowing from anticipated fraud and  
22 identity theft posed by his Private Information being placed in the hands of  
23 cybercriminals; (iii) damages to and diminution in value of his Private Information  
24 that was entrusted to Defendants with the understanding that Defendants would  
25 safeguard this information against disclosure; (iv) loss of the benefit of the bargain  
26 with Defendants to provide adequate and reasonable data security—*i.e.*, the  
27

1 difference in value between what Plaintiff Kyle McDaniel should have received  
2 from Defendants and Defendants' defective and deficient performance of that  
3 obligation by failing to provide reasonable and adequate data security and failing to  
4 protect his Private Information; and (v) continued risk to his Private Information,  
5 which remains in the possession of Defendants and which is subject to further  
6 breaches so long as Defendants fails to undertake appropriate and adequate measures  
7 to protect the Private Information that was entrusted to Defendants.

8 ***Plaintiff Rikki McDaniel***

9 127. Plaintiff Rikki McDaniel received a Notice of Data Breach Letter from  
10 TGCS informing her that her highly confidential Private Information was  
11 compromised in the Data Breach.

12 128. Plaintiff Rikki McDaniel's PII was provided to TGCS to receive  
13 benefits stemming from her husband's employment at TGCS.

14 129. Defendants were in possession of Plaintiff Rikki McDaniel's Private  
15 Information before, during, and after the Data Breach.

16 130. Because of the Data Breach, there is no doubt Plaintiff Rikki  
17 McDaniel's highly confidential Private Information is in the hands of  
18 cybercriminals. Reason being, the Notice of Data Breach Letter from TGCS  
19 disclosed that an unauthorized third-party accessed Defendants' system. The *modus*  
20 *operandi* of cybercriminals involves stealing Private Information for financial gain.  
21 Cybercriminals may use stolen identities to conceal their own true identity or carry  
22 out a range of fraudulent activities, from credit card fraud to impersonation. As such,  
23 Plaintiff Rikki McDaniel and the Class are at an imminent risk of identity theft and  
24 fraud.

25 131. As a result of the Data Breach, Plaintiff Rikki McDaniel has already  
26 expended over **100 hours** of her time and has suffered loss of productivity from  
27



1 taking time to address and attempt to ameliorate, mitigate, and address the future  
2 consequences of the Data Breach. This includes: (i) investigating the Data Breach;  
3 (ii) investigating how best to ensure that she is protected from identity theft; and (iii)  
4 reviewing her account statements, credit reports, and/or other information.

5 132. Plaintiff Rikki McDaniel places significant value in the security of her  
6 Private Information and does not readily disclose it. Plaintiff Rikki McDaniel has  
7 never knowingly transmitted unencrypted Private Information over the internet or  
8 any other unsecured source.

9 133. Plaintiff Rikki McDaniel has been and will continue to be at a  
10 heightened and substantial risk of future identity theft and its attendant damages for  
11 years to come. Such a risk is certainly real and impending, and is not speculative,  
12 given the highly sensitive nature of the Private Information compromised by the  
13 Data Breach. Indeed, Defendants acknowledged the present and increased risk of  
14 future harm Plaintiff Rikki McDaniel, and the Class now face by offering temporary,  
15 non-automatic credit monitoring services to Plaintiff Rikki McDaniel and the Class.

16 134. Knowing that thieves intentionally targeted and stole her Private  
17 Information, including her Social Security number, and knowing that her Private  
18 Information is in the hands of cybercriminals has caused Plaintiff Rikki McDaniel  
19 great anxiety beyond mere worry. Specifically, Plaintiff Rikki McDaniel has lost  
20 hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of  
21 persistent worry now that her Private Information has been stolen.

22 135. Plaintiff Rikki McDaniel has a continuing interest in ensuring that her  
23 Private Information, which, upon information and belief, remains in the possession  
24 of Defendants, is protected, and safeguarded from future data breaches. Absent  
25 Court intervention, Plaintiff Rikki McDaniels' and the Class's Private Information  
26 will be wholly unprotected and at-risk of future data breaches.

1           136. Plaintiff Rikki McDaniel has suffered injuries directly and proximately  
2 caused by the Data Breach, including: (i) theft of her valuable Private Information;  
3 (ii) the imminent and certain impending injury flowing from anticipated fraud and  
4 identity theft posed by her Private Information being placed in the hands of  
5 cybercriminals; (iii) damages to and diminution in value of her Private Information  
6 that was entrusted to Defendants with the understanding that Defendants would  
7 safeguard this information against disclosure; (iv) loss of the benefit of the bargain  
8 with Defendants to provide adequate and reasonable data security—*i.e.*, the  
9 difference in value between what Plaintiff Rikki McDaniel should have received  
10 from Defendants and Defendants’ defective and deficient performance of that  
11 obligation by failing to provide reasonable and adequate data security and failing to  
12 protect her Private Information; and (v) continued risk to her Private Information,  
13 which remains in the possession of Defendants and which is subject to further  
14 breaches so long as Defendants fails to undertake appropriate and adequate measures  
15 to protect the Private Information that was entrusted to Defendants.

16 ***Plaintiff Jon Williams***

17           137. Plaintiff Jon Williams received a Notice of Data Breach Letter from  
18 TGCS informing him that his highly confidential Private Information was  
19 compromised in the Data Breach.

20           138. Plaintiff Jon Williams is a former employee of Toshiba.

21           139. Defendants were in possession of Plaintiff Jon Williams’ Private  
22 Information before, during, and after the Data Breach.

23           140. Because of the Data Breach, there is no doubt Plaintiff Jon Williams’  
24 highly confidential Private Information is in the hands of cybercriminals. Reason  
25 being, the Notice of Data Breach Letter from TGCS disclosed that an unauthorized  
26 third-party accessed Defendants’ system. The *modus operandi* of cybercriminals  
27  
28

1 involves stealing Private Information for financial gain. Cybercriminals may use  
2 stolen identities to conceal their own true identity or carry out a range of fraudulent  
3 activities, from credit card fraud to impersonation. As such, Plaintiff Jon Williams  
4 and the Class are at imminent risk of identity theft and fraud.

5 141. As a result of the Data Breach, Plaintiff Jon Williams has already  
6 expended at least 7 hours of his time and has suffered loss of productivity from  
7 taking time to address and attempt to ameliorate, mitigate, and address the future  
8 consequences of the Data Breach. This includes: (i) investigating the Data Breach;  
9 (ii) investigating how best to ensure that he is protected from identity theft; and (iii)  
10 reviewing his account statements, credit reports, and/or other information.

11 142. Plaintiff Jon Williams places significant value on the security of his  
12 Private Information and does not readily disclose it. Plaintiff Jon Williams has never  
13 knowingly transmitted unencrypted Private Information over the internet or any  
14 other unsecured source.

15 143. Plaintiff Jon Williams has been and will continue to be at a heightened  
16 and substantial risk of future identity theft and its attendant damages for years to  
17 come. Such a risk is certainly real and impending, and is not speculative, given the  
18 highly sensitive nature of the Private Information compromised by the Data Breach.  
19 Indeed, Defendants acknowledged the present and increased risk of future harm  
20 Plaintiff Jon Williams, and the Class now face by offering temporary, non-automatic  
21 credit monitoring services to Plaintiff Jon Williams and the Class.

22 144. Knowing that thieves intentionally targeted and stole his Private  
23 Information, including his Social Security number, and knowing that his Private  
24 Information is in the hands of cybercriminals has caused Plaintiff Jon Williams great  
25 anxiety beyond mere worry. Specifically, Plaintiff Jon Williams has lost hours of  
26  
27  
28

1 sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent  
2 worry now that his Private Information has been stolen.

3 145. Plaintiff Jon Williams has a continuing interest in ensuring that his  
4 Private Information, which, upon information and belief, remains in the possession  
5 of Defendants, is protected, and safeguarded from future data breaches. Absent  
6 Court intervention, Plaintiff Jon Williams' and the Class's Private Information will  
7 be wholly unprotected and at-risk of future data breaches.

8 146. Plaintiff Jon Williams has suffered injuries directly and proximately  
9 caused by the Data Breach, including: (i) theft of his valuable Private Information;  
10 (ii) the imminent and certain impending injury flowing from anticipated fraud and  
11 identity theft posed by his Private Information being placed in the hands of  
12 cybercriminals; (iii) damages to and diminution in value of his Private Information  
13 that was entrusted to Defendants with the understanding that Defendants would  
14 safeguard this information against disclosure; (iv) loss of the benefit of the bargain  
15 with Defendants to provide adequate and reasonable data security—i.e., the  
16 difference in value between what Plaintiff Jon Williams should have received from  
17 Defendants and Defendants' defective and deficient performance of that obligation  
18 by failing to provide reasonable and adequate data security and failing to protect his  
19 Private Information; and (v) continued risk to his Private Information, which remains  
20 in the possession of Defendants and which is subject to further breaches so long as  
21 Defendants fails to undertake appropriate and adequate measures to protect the  
22 Private Information that was entrusted to Defendants.

23 ***Plaintiff Mojdeh Williams***

24 147. Plaintiff Mojdeh Williams received a Notice of Data Breach Letter  
25 from TGCS informing her that her highly confidential Private Information was  
26 compromised in the Data Breach.

1 148. Plaintiff Mojdeh Williams's PII was provided to TGCS to receive  
2 benefits stemming from her husband's employment at TGCS.

3 149. Defendants were in possession of Plaintiff Mojdeh Williams' Private  
4 Information before, during, and after the Data Breach.

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

14 151. As a result of the Data Breach, Plaintiff Mojdeh Williams has already  
15 expended at least **6 hours** of her time and has suffered loss of productivity from  
16 taking time to address and attempt to ameliorate, mitigate, and address the future  
17 consequences of the Data Breach. This includes: (i) investigating the Data Breach;  
18 (ii) investigating how best to ensure that she is protected from identity theft; and (iii)  
19 reviewing her account statements, credit reports, and/or other information.

20 152. Due to the imminent risk of harm stemming from the Data Breach  
21 Plaintiff Mojdeh Williams froze her credit (which caused further inconvenience and  
22 damage in that Plaintiff Mojdeh Williams is now deprived of access to her own  
23 credit).

24 153. Plaintiff Mojdeh Williams places significant value in the security of her  
25 Private Information and does not readily disclose it. Plaintiff Mojdeh Williams has  
26  
27  
28

1 never knowingly transmitted unencrypted Private Information over the internet or  
2 any other unsecured source.

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

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

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

22 157. Plaintiff Mojdeh Williams has suffered injuries directly and  
23 proximately caused by the Data Breach, including: (i) theft of her valuable Private  
24 Information; (ii) the imminent and certain impending injury flowing from  
25 anticipated fraud and identity theft posed by her Private Information being placed in  
26 the hands of cybercriminals; (iii) damages to and diminution in value of her Private  
27

Information that was entrusted to Defendants with the understanding that Defendants would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendants to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Mojdeh Williams should have received from Defendants and Defendants’ defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect her Private Information; and (v) continued risk to her Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

#### **V. CLASS ACTION ALLEGATIONS**

158. Plaintiffs incorporate by reference all preceding paragraphs as if fully restated here.

159. Plaintiffs bring this action against Toshiba on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide class (the “Class”) defined as follows:

**All persons who were sent a Notice of Data Breach Letter from TGCS or TABS.**

160. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants’ officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

161. Plaintiffs reserve the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.



1           162. Plaintiffs anticipate the issuance of notice setting forth the subject and  
2 nature of the instant action to the proposed Class. Upon information and belief,  
3 Defendants' own business records or electronic media can be utilized for the notice  
4 process.

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

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

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

15           166. **Adequacy:** Plaintiffs are adequate representatives of the Class because  
16 Plaintiffs' interests do not conflict with the interests of the Class; Plaintiffs have  
17 retained counsel competent and highly experienced in data breach class action  
18 litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action  
19 vigorously. The interests of the Class will be fairly and adequately protected by  
20 Plaintiffs and their counsel.

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



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

168. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs 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 Defendants engaged in the wrongful conduct alleged herein;
- b. Whether Defendants failed to adequately safeguard Plaintiffs' and the Class's PII;
- c. Whether Defendants owed a duty to Plaintiffs and the Class to adequately protect their PII, and whether it breached this duty;
- d. Whether Toshiba breached its duties to Plaintiffs and the Class;
- e. Whether Toshiba failed to provide adequate cybersecurity;
- f. Whether Toshiba knew or should have known that its email accounts and network security systems were vulnerable to cyberattacks;
- 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 email accounts;
- i. Whether Toshiba was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees and their dependents;

- 1 j. Whether Toshiba breached implied contractual duties to Plaintiffs 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 Plaintiffs and  
7 the Class;
- 8 l. Whether Toshiba continues to breach duties to Plaintiffs and the Class;
- 9 m. Whether Plaintiffs and the Class suffered injury as a proximate result  
10 of Toshiba's negligent actions or failures to act;
- 11 n. Whether Plaintiffs 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 Plaintiffs 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 Plaintiffs and the Class)**

20 169. Plaintiffs incorporate paragraphs 1–168 as though fully set forth herein.

21 170. Toshiba solicited, gathered, and stored the PII of Plaintiffs and Class  
22 Members.

23 171. Upon accepting and storing the PII of Plaintiffs and Class members on  
24 their computer systems and networks, Defendants undertook and owed a duty to  
25 Plaintiffs and Class members to exercise reasonable care in obtaining, retaining,  
26 securing, safeguarding, deleting, and protecting the PII of Plaintiffs and the Class  
27 from being compromised, lost, stolen, accessed, and misused by unauthorized

1 persons.

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

8 173. Because of this special relationship, Defendants required Plaintiffs and  
9 Class members to provide their PII, including names, Social Security numbers, and  
10 other PII.

11 174. Implied in these exchanges was a promise by Defendants to ensure that  
12 the PII of Plaintiffs and Class members in their possession was only used for the  
13 provided purpose and that Defendants would destroy any PII that it was not required  
14 to maintain.

15 175. As part of this special relationship, Defendants had a duty to perform  
16 with skill, care, and reasonable expedience and faithfulness.

17 176. Through Defendants' acts and omissions, including Defendants' failure  
18 to provide adequate data security, their failure to protect Plaintiffs' and Class  
19 members' PII from being foreseeably accessed, and their improper retention of PII  
20 they was not required to maintain, Defendants negligently failed to observe and  
21 perform their duty.

22 177. Plaintiffs and Class members did not receive the benefit of the bargain  
23 with Defendants, because providing their PII was in exchange for Defendants'  
24 implied agreement to secure and keep it safe and to delete it once no longer required.

25 178. Defendants knew cybercriminals routinely target large corporations  
26 through cyberattacks to steal customer and employee PII. In other words, Defendants  
27

1 knew of a foreseeable risk to their data security systems but failed to implement  
2 reasonable security measures.

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

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

14 181. Defendants had duties to protect and safeguard the PII of Plaintiffs and  
15 the Class from being vulnerable to cyberattacks by taking common-sense  
16 precautions when dealing with sensitive PII. Additional duties that Defendants owed  
17 Plaintiffs, and the Class include:

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

1 c. To implement processes to quickly detect a data breach, security  
2 incident, or intrusion involving their networks, servers, and email  
3 accounts; and

4 d. To promptly notify Plaintiffs and Class members of any data breach,  
5 security incident, or intrusion that affected or may have affected their  
6 PII.

7 182. Plaintiffs and the Class were the intended beneficiaries of Defendants'  
8 duties, creating a special relationship between them and Defendants. Defendants  
9 were in a position to ensure that their systems were sufficient to protect the PII that  
10 Plaintiffs and the Class had entrusted to it.

11 183. Plaintiffs' injuries and damages, as described herein, are a reasonably  
12 certain consequence of Defendants' negligence and breach of their duties.

13 184. Defendants breached their duties of care by failing to adequately protect  
14 Plaintiffs' and Class members' PII. Defendants breached their duties by, among  
15 other things:

16 a. Failing to exercise reasonable care in obtaining, retaining securing,  
17 safeguarding, and protecting the PII in their possession;

18 b. Failing to protect the PII in their possession using reasonable and  
19 adequate security procedures and systems;

20 c. Failing to consistently enforce security policies aimed at protecting  
21 Plaintiffs and the Class's PII;

22 d. Failing to implement processes to quickly detect data breaches, security  
23 incidents, phishing incidents, or intrusions;

24 e. Failing to promptly notify Plaintiffs and Class members of the Data  
25 Breach that affected their PII.

1 185. Defendants' willful failure to abide by these duties was wrongful,  
2 reckless, and grossly negligent considering the foreseeable risks and known threats.

3 186. As a direct and proximate result of Defendants' negligent conduct,  
4 including but not limited to their failure to implement and maintain reasonable data  
5 security practices and procedures as described above, Plaintiffs and the Class have  
6 suffered damages and are at imminent risk of additional harms and damages (as  
7 alleged above).

8 187. Through Defendants' acts and omissions described herein, including  
9 but not limited to Defendants' failure to protect the PII of Plaintiffs and Class  
10 members from being stolen and misused, Defendants unlawfully breached their duty  
11 to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class  
12 members while it was within Defendants' possession and control.

13 188. Further, through their failure to provide timely and clear notification of  
14 the Data Breach to Plaintiffs and Class members, Defendants prevented Plaintiffs  
15 and Class members from taking meaningful, proactive steps to securing their PII and  
16 mitigating damages.

17 189. Plaintiffs and Class members could have taken actions earlier had they  
18 been timely notified of the Data Breach, rather than months after it occurred.

19 190. Plaintiffs and Class members could have enrolled in credit monitoring,  
20 could have instituted credit freezes, and could have changed their passwords, among  
21 other things, had they been alerted to the Data Breach more quickly.

22 191. Plaintiffs and Class members have suffered harm from the delay in  
23 notifying them of the Data Breach.

24 192. As a direct and proximate cause of Defendants' conduct, including but  
25 not limited to their failure to implement and maintain reasonable security practices  
26 and procedures, Plaintiffs and Class members have suffered, as Plaintiffs have,  
27

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

20 193. The damages Plaintiffs and the Class have suffered (as alleged above)  
21 and will suffer were and are the direct and proximate result of Defendants' negligent  
22 conduct.

23 194. Plaintiffs and the Class have suffered injury and are entitled to actual  
24 and punitive damages in an amount to be proven at trial.  
25  
26  
27

**SECOND CAUSE OF ACTION**  
**NEGLIGENCE *PER SE***  
**(On Behalf of Plaintiffs and the Class)**

195. Plaintiffs incorporates paragraphs 1–168 as though fully set forth herein.

196. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendants had a duty to Plaintiffs and the Class to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and the Class.

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

198. Defendants gathered and stored the PII of Plaintiffs and the Class as part of Defendants’ business which affects commerce.

199. Defendants violated the FTC Act by failing to use reasonable measures to protect the PII of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

200. Defendants breached their duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs’ and Class members’ PII, and by failing to provide prompt notice without reasonable delay.

201. Defendants’ multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

202. Plaintiffs and the Class are within the class of persons that the FTC Act was intended to protect.

203. The harm that occurred as a result of the Data Breach is the type of



1 harm the FTC Act was intended to guard against.

2 204. Defendants breached their duties to Plaintiffs and the Class under the  
3 FTC Act by failing to provide fair, reasonable, or adequate computer systems and  
4 data security practices to safeguard Plaintiffs' and the Class's PII.

5 205. Defendants breached their duties to Plaintiffs and the Class by  
6 unreasonably delaying and failing to provide notice of the Data Breach expeditiously  
7 and/or as soon as practicable to Plaintiffs and the Class.

8 206. Defendants' violations of the FTC Act constitute negligence *per se*.

9 207. As a direct and proximate result of Defendants' negligence *per se*,  
10 Plaintiffs and the Class have suffered, and continue to suffer, damages arising from  
11 the Data Breach, as alleged above.

12 208. The injury and harm that Plaintiffs and Class members suffered (as  
13 alleged above) was the direct and proximate result of Defendants' negligence *per se*.

14 209. Plaintiffs and the Class have suffered injury and are entitled to damages  
15 in amounts to be proven at trial.

16 **THIRD CAUSE OF ACTION**  
17 **BREACH OF IMPLIED CONTRACT**  
**(On Behalf of Plaintiffs and the Class)**

18 210. Plaintiffs incorporate paragraphs 1–168 as though fully set forth herein.

19 211. Toshiba required Plaintiffs and Class Members to provide and entrust  
20 their Private Information to Toshiba as a condition of obtaining Toshiba's services,  
21 benefits, and employment.

22 212. When Plaintiffs and Class Members provided their Private Information  
23 to Toshiba, they entered into implied contracts with Toshiba pursuant to which  
24 Toshiba agreed, as manifested through their conduct, to safeguard and protect such  
25 Private Information and to timely and accurately notify Plaintiffs and Class  
26 Members if and when their Private Information was breached and compromised.

1           213. Specifically, Plaintiffs and Class Members entered into valid and  
2 enforceable implied contracts with Toshiba when they agreed to provide their  
3 Private Information and/or payment to Toshiba, and Toshiba agreed to collect,  
4 maintain, and profit from that Private Information.

5           214. The valid and enforceable implied contracts that Plaintiffs and Class  
6 Members entered into with Toshiba included Toshiba's promises to protect Private  
7 Information it collected from Plaintiffs and Class Members against unauthorized  
8 disclosures. Plaintiffs and Class Members provided this Private Information in  
9 reliance on Toshiba's promises.

10           215. Under the implied contracts, Toshiba promised and was obligated to  
11 protect Plaintiffs' and Class Members' Private Information provided to obtain  
12 Toshiba's services and/or employment. In exchange, Plaintiffs and Class Members  
13 agreed to provide Toshiba with their Private Information.

14           216. Toshiba promised and warranted to Plaintiffs and Class Members,  
15 through privacy documents and conduct, to maintain the privacy and confidentiality  
16 of the Private Information it collected from Plaintiffs and Class Members and to  
17 keep such information safeguarded against unauthorized access and disclosure.

18           217. Toshiba's adequate protection of Plaintiffs' and Class Members'  
19 Private Information was a material aspect of these implied contracts with Toshiba.

20           218. Toshiba solicited and invited Plaintiffs and Class Members to provide  
21 their Private Information as part of Toshiba's regular business practices. Plaintiffs  
22 and Class Members accepted Toshiba's offers and provided their Private  
23 Information to Toshiba.

24           219. In entering into such implied contracts, Plaintiffs and Class Members  
25 reasonably believed and expected that Toshiba's data security practices complied  
26 with industry standards and relevant laws and regulations, including the FTC Act.  
27

1           220. Plaintiffs and Class Members provided their Private Information to  
2 Toshiba reasonably believed and expected that Toshiba would adequately employ  
3 adequate data security to protect that Private Information. Toshiba failed to do so.

4           221. A meeting of the minds occurred when Plaintiffs and Class Members  
5 agreed to, and did, provide their Private Information to Toshiba and agreed Toshiba  
6 would receive payment for and benefit from, amongst other things, the protection of  
7 their Private Information.

8           222. Plaintiffs and Class Members performed their obligations under the  
9 contracts when they provided their Private Information and/or payment to Toshiba.

10          223. Toshiba materially breached its contractual obligations to protect the  
11 Private Information it required Plaintiffs and Class Members to provide when that  
12 Private Information was unauthorizedly disclosed in the Data Breach due to  
13 Toshiba's inadequate data security measures and procedures.

14          224. Toshiba materially breached its contractual obligations to deal in good  
15 faith with Plaintiffs and Class Members when it failed to take adequate precautions  
16 to prevent the Data Breach, and when it failed to timely or adequately notify  
17 Plaintiffs and Class Members about the Data Breach.

18          225. The Data Breach was a reasonably foreseeable consequence of  
19 Toshiba's conduct, by acts of omission or commission, in breach of these implied  
20 contracts with Plaintiffs and Class Members.

21          226. As a result of Toshiba's failures to fulfill the data security protections  
22 promised in these contracts, Plaintiffs and Class Members did not receive the full  
23 benefit of their bargains with Toshiba, and instead received services of a diminished  
24 value compared to that described in the implied contracts. Plaintiffs and Class  
25 Members were therefore damaged in an amount at least equal to the difference in the  
26  
27  
28

1 value of the services with data security protection they paid for and that which they  
2 received.

3 227. Had Toshiba disclosed that their data security procedures were  
4 inadequate or that they did not adhere to industry-standard for cybersecurity, neither  
5 Plaintiffs, Class Members, nor any reasonable person would have contracted with  
6 Toshiba.

7 228. Plaintiffs and Class Members would not have provided and entrusted  
8 their Private Information to Toshiba in the absence of the implied contracts between  
9 them and Toshiba.

10 229. Plaintiffs and Class Members fully performed their obligations under  
11 the implied contracts with Toshiba.

12 230. Plaintiffs and Class Members are entitled to damages, including  
13 compensatory, punitive, and/or restitution damages, in an amount to be proven at  
14 trial, due to Toshiba's breach of implied contract.

15 **FOURTH CAUSE OF ACTION**  
16 **UNJUST ENRICHMENT**  
**(On Behalf of Plaintiffs and the Class)**

17 231. Plaintiffs incorporate paragraphs 1–168 as though fully set forth herein.

18 232. Plaintiffs allege this claim in the alternative to his breach of implied  
19 contract claim.

20 233. Defendants knew that Plaintiffs and Class Members conferred a benefit  
21 upon it and accepted and retained that benefit by accepting and retaining the PII  
22 entrusted to it. Defendants profited from Plaintiffs' retained data and  
23 commercialized and used Plaintiffs' and Class Members' PII for business purposes.

24 234. Upon information and belief, Defendants funds their data security  
25 measures entirely from their general revenue, including payments on behalf of or for  
26 the benefit of Plaintiffs and Class Members.

1           235. As such, a portion of the payments made for the benefit of or on behalf  
2 of Plaintiffs and Class Members is to be used to provide a reasonable level of data  
3 security, and the amount of the portion of each payment made that is allocated to  
4 data security is known to Defendants.

5           236. Defendants failed to secure Plaintiffs' and Class Members' Private  
6 Information and, therefore, did not fully compensate Plaintiffs or Class Members for  
7 the value that their PII provided.

8           237. Defendants acquired the PII through inequitable means as it failed to  
9 disclose the inadequate data security practices previously alleged. If Plaintiffs and  
10 Class Members had known that Defendants would not fund adequate data security  
11 practices, procedures, and protocols to sufficiently monitor, supervise, and secure  
12 their PII, they would not have entrusted their Private Information to Defendants or  
13 obtained services from Defendants' clients.

14           238. Defendants enriched themselves by saving the costs it reasonably  
15 should have expended on data security measures to secure Plaintiffs' and Class  
16 Members' PII. Instead of providing a reasonable level of security that would have  
17 prevented the Data Breach, Defendants instead calculated to increase their own  
18 profits at the expense of Plaintiffs and Class Members by utilizing cheaper,  
19 ineffective security measures and diverting those funds to their own benefit.  
20 Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate  
21 result of Defendants' decision to prioritize their own profits over the requisite  
22 security and the safety of their PII.

23           239. Plaintiffs and Class Members have no adequate remedy at law.

24           240. Under the circumstances, it would be unjust for Defendants to be  
25 permitted to retain any of the benefits that Plaintiffs and Class Members conferred  
26 upon it.

1           241. As a direct and proximate result of Defendants' conduct, Plaintiffs and  
2 other Class Members, have suffered actual harm in the form of experiencing specific  
3 acts of fraudulent activity and other attempts of fraud that required Plaintiffs' efforts  
4 to prevent from succeeding.

5           242. As a result of Defendants' wrongful conduct, as alleged above,  
6 Plaintiffs and the Class are entitled to restitution and disgorgement of profits,  
7 benefits, and other compensation obtained by Defendants and all other relief allowed  
8 by law.

9                           **FIFTH CAUSE OF ACTION**  
10                          **DECLARATORY AND INJUNCTIVE RELIEF**  
11                          **(On Behalf of Plaintiffs and the Class)**

12           243. Plaintiffs incorporate paragraphs 1–168 as though fully set forth herein.

13           244. This count is brought under the Federal Declaratory Judgment Act, 28  
14 U.S.C. § 2201.

15           245. As previously alleged, Plaintiffs and members of the Class are entered  
16 into implied contracts with Defendants, which contracts require Defendants to  
17 provide adequate security for the PII collected from Plaintiffs and the Class.

18           246. Defendants owed and still owes a duty of care to Plaintiffs and Class  
19 members that require it to adequately secure Plaintiffs' and Class members' PII.

20           247. Upon reason and belief, Defendants still possesses the PII of Plaintiffs  
21 and the Class members.

22           248. Defendants has not satisfied their contractual obligations and legal  
23 duties to Plaintiffs and the Class members.

24           249. Since the Data Breach, Defendants have not yet announced any changes  
25 to their data security infrastructure, processes or procedures to fix the vulnerabilities  
26 in their computer systems and/or security practices which permitted the Data Breach  
27 to occur and go undetected and, thereby, prevent further attacks.

1           250. Defendants has not satisfied their contractual obligations and legal  
2 duties to Plaintiffs and the Class. In fact, now that Defendants' insufficient data  
3 security is known to hackers, the PII in Defendants' possession is even more  
4 vulnerable to cyberattack.

5           251. Actual harm has arisen in the wake of the Data Breach regarding  
6 Defendants' contractual obligations and duties of care to provide security measures  
7 to Plaintiffs and the members of the Class. Further, Plaintiffs and the members of  
8 the Class are at risk of additional or further harm due to the exposure of their PII and  
9 Defendants' failure to address the security failings that led to such exposure.

10           252. There is no reason to believe that Defendants' security measures are  
11 any more adequate now than they were before the Data Breach to meet Defendants'  
12 contractual obligations and legal duties.

13           253. Plaintiffs and the Class, therefore, seek a declaration (1) that  
14 Defendants' existing security measures do not comply with their contractual  
15 obligations and duties of care to provide adequate security, and (2) that to comply  
16 with their contractual obligations and duties of care, Defendants must implement  
17 and maintain reasonable security measures, including, but not limited to:

- 18           a. Ordering that Defendants engage third-party security  
19           auditors/penetration testers as well as internal security personnel to  
20           conduct testing, including simulated attacks, penetration tests, and  
21           audits on Defendants' systems on a periodic basis, and ordering  
22           Defendants to promptly correct any problems or issues detected by  
23           such third-party security auditors;
- 24           b. Ordering that Defendants engage third-party security auditors and  
25           internal personnel to run automated security monitoring;
- 26           c. Ordering that Defendants audit, test, and train their security  
27

- 1 personnel regarding any new or modified procedures;
- 2 d. Ordering that Defendants segment employee data by, among other
- 3 things, creating firewalls and access controls so that if one area of
- 4 Defendants' systems is compromised, hackers cannot gain access to
- 5 other portions of Defendants' systems;
- 6 e. Ordering that Defendants purge, delete, and destroy, in a reasonably
- 7 secure manner, customer data not necessary for their provisions of
- 8 services;
- 9 f. Ordering that Defendants conduct regular database scanning and
- 10 security checks; and
- 11 g. Ordering that Defendants routinely and continually conduct internal
- 12 training and education to inform internal security personnel how to
- 13 identify and contain a breach when it occurs and what to do in
- 14 response to a breach.

15 **VI. PRAYER FOR RELIEF**

16 WHEREFORE, Plaintiffs and the Class pray for judgment against

17 Defendants as follows:

- 18 a. An order certifying this action as a class action under Federal Rule
- 19 of Civil Procedure 23, defining the Class as requested herein,
- 20 appointing the undersigned as Class counsel, and finding that
- 21 Plaintiffs are proper representatives of the Class requested herein;
- 22 b. A judgment in favor of Plaintiffs and the Class awarding them
- 23 appropriate monetary relief, including compensatory damages,
- 24 punitive damages, attorney fees, expenses, costs, and such other and
- 25 further relief as is just and proper;
- 26
- 27



- 1 c. An order providing injunctive and other equitable relief as necessary  
2 to protect the interests of the Class as requested herein;  
3 d. An order requiring Defendants to pay the costs involved in notifying  
4 the Class Members about the judgment and administering the claims  
5 process;  
6 e. A judgment in favor of Plaintiffs and the Class awarding them pre-  
7 judgment and post-judgment interest, reasonable attorneys' fees,  
8 costs, and expenses as allowable by law; and  
9 f. An award of such other and further relief as this Court may deem  
10 just and proper.

11 **II. DEMAND FOR JURY TRIAL**

12 Plaintiffs hereby demands a trial by jury on all appropriate issues raised in  
13 this Amended Class Action Complaint.

14 Dated: December 10, 2024

Respectfully submitted,

16 /s/: William B. Federman

William B. Federman

(pro hac vice)

Kennedy M. Brian

(pro hac vice)

19 **FEDERMAN & SHERWOOD**

10205 N. Pennsylvania Ave.

Oklahoma City, OK 73120

21 T: (405) 235-1560

22 F: (405) 239-2112

E: wbf@federmanlaw.com

23 E: [kpb@federmanlaw.com](mailto:kpb@federmanlaw.com)

24 Byron T. Ball

25 (State Bar No. 150195)

26 **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

# EXHIBIT 1



# TOSHIBA



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.

# EXHIBIT 2



# TOSHIBA



4\_0000638

November 26, 2024

RIKKI J MCDANIEL  


Dear Rikki 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 secure our email tenant. Through the investigation, we learned that your name and Social Security number were potentially 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 in 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) 676-6412 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.

# EXHIBIT 3





# TOSHIBA



3\_0000588

July 23, 2024

JON WILLIAMS  


Dear Jon Williams:

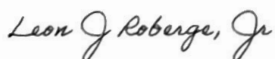
Toshiba Global Commerce Solutions, Inc. is committed to protecting the confidentiality and security of the personal information we maintain. I am writing to inform you of a data security incident that potentially involved some of your information. This notice explains the incident, the measures we have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



# EXHIBIT 4

# TOSHIBA



3\_0000375

November 26, 2024

MOJDEH WILLIAMS  


Dear Mojdeh Williams:

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 secure our email tenant. Through the investigation, we learned that your name and Social Security number were potentially 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 in 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) 676-6412 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.