Andrew G. Gunem (SBN 354042)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Ste. 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com

Attorneys for Plaintiff and Proposed Class
[Additional Counsel on Signature Page]

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

EASTERN DIVISION

KYLE MCDANIEL, RIKKI MCDANIEL, JON WILLIAMS, MOJDEH WILLIAMS, and **TOM SIMMONS,** on behalf of themselves and all similarly situated individuals,

Plaintiffs,

v.

TOSHIBA GLOBAL COMMERCE SOLUTIONS, INC.,

Defendant.

Case No.: 8:24-cv-01772

Hon. Fred W. Slaughter

SECOND AMENDED CLASS ACTION COMPLAINT

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

JURY TRIAL DEMANDED

Plaintiffs Kyle McDaniel, Rikki McDaniel, Jon Williams, Mojdeh Williams, and Tom Simmons (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 Second Amended Class

Action Complaint against Toshiba Global Commerce Solutions, Inc., ("TGCS," "Toshiba," or "Defendant")[1] and allege the following based on personal knowledge of facts, upon information and belief, and based on the investigation of their counsel as to all other matters.

I. INTRODUCTION

1. Plaintiffs bring this class action lawsuit against Toshiba for its failure to protect Plaintiffs' and the Class's highly sensitive personally identifiable information ("PII") from hackers.[2] As a result of Toshiba's inadequate data security, cybercriminals easily infiltrated Defendant's inadequately protected email accounts and accessed the PII of Plaintiffs and the Class (the "Data Breach" or "Breach").[3] Now, Plaintiffs' and the Class's PII is in the hands of cybercriminals who will sell their PII on the dark web and use their PII for nefarious purposes for the rest of their lives.

2. On an undisclosed date, Toshiba discovered suspicious activity within its email environment.[4] After an investigation, it was determined that an unknown and unauthorized threat actor hacked into Toshiba's inadequately secured email environment between December 4, 2023, through March 18, 2024. Thus, the hacker(s) had access to Toshiba's email accounts—and Plaintiffs' and the Class's

[1] TGCS was inadvertently named as "Toshiba Global Commerce Solutions" instead of "Toshiba Global Commerce Solutions, Inc." in Plaintiffs' First Amended Complaint.

[2] OFFICE OF THE MAINE ATTORNEY GENERAL, *Toshiba Global Commerce Solutions*, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8fea1aeb-d918-4c0d-b40d-97990f1eb395.html.

[3] *Id.*

[4] *Id.*

PII contained therein—for ***over three (3) months***.[5]

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

4. The PII accessed in the Data Breach included highly sensitive PII such as, names and Social Security numbers, (collectively, "Private Information").[7]

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

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

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

---

[5] *Id.*
[6] *Id.*
[7] *Id.*

8. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Toshiba assumed legal and equitable duties to Plaintiffs and the Class. Businesses that handle consumers' and employees' Private Information, like Toshiba, owe the individuals to whom the information relates a duty to adopt reasonable measures to protect it from disclosure to and theft by unauthorized third parties, and to keep it safe and confidential. This duty arises under contract, statutory and common law, industry standards, representations made to Plaintiffs and Class Members, and because it is foreseeable that hackers with nefarious intentions will target the Private Information and use it to harm the affected individuals.

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

10. The Data Breach, which Toshiba failed to detect until cybercriminals had already accessed, viewed, and stolen Plaintiffs' and Class Members' Private Information, is the direct result of Toshiba's failure to implement basic data security

measures or oversight over Plaintiffs' and the Class's PII in its custody and control. Had Toshiba implemented reasonable cybersecurity measures—including adequate safeguards for initial access, encryption or redaction of personal data elements, and sufficient logging, monitoring, and alerting tools to detect unauthorized activity—criminals would not have been able to hack into Toshiba's email accounts, perform reconnaissance necessary to locate Plaintiffs' and Class Members' Private Information, and then access that data before being detected. The fact that Toshiba failed to detect the Breach for ***months*** is direct evidence of its negligence to implement industry standard data security measures.

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

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

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

personal lives of thousands of individuals.

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

15. The harm resulting from a data breach like this manifests in numerous ways including identity theft and financial fraud, and the exposure of an individual's Private Information due to breach ensures that the individual will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of his or her life. Mitigating that risk, to the extent even possible, requires individuals to devote significant time and money to closely monitor their credit, financial accounts, and email accounts, and take several additional prophylactic measures. Plaintiffs and Class Members will be forced to allocate time to these tasks for years, if not their lifetimes, due to Toshiba's Data Breach.

16. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries in fact including, but not limited to: (i) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (ii) loss of

time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (iii) actual identity theft and fraud; (iv) financial costs incurred due to actual identity theft; (v) loss of time incurred due to actual identity theft; (vi) deprivation of value of their Private Information; (vii) loss of privacy; (viii) emotional distress including anxiety and stress in with dealing with the Data Breach; and (ix) the continued risk to their sensitive Private Information, which remains in Toshiba's possession and subject to further data breaches, so long as Toshiba fails to undertake appropriate and adequate measures to protect the consumer data it collects and maintains.

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

18. To recover for these harms, Plaintiffs, on behalf of themselves and the Class as defined herein, bring claims for negligence/negligence per se, breach of implied contract, unjust enrichment, and declaratory/injunctive relief, to address Toshiba's inadequate safeguarding of Plaintiffs' and Class Members' Private Information in its custody and Toshiba's failure to provide timely or adequate notice to Plaintiffs and Class Members that their information was compromised in the Data Breach.

19. Plaintiffs and Class Members seek compensatory, nominal, statutory, and punitive damages, declaratory judgment, and injunctive relief requiring Toshiba to: (i) disclose, expeditiously, the full nature of the Data Breach and the types of Private Information exposed; (ii) implement improved data security practices to

reasonably guard against future breaches of Private Information in Toshiba's possession; and (iii) provide, at Toshiba's own expense, all impacted Data Breach victims with lifetime identity theft protection services.

II. THE PARTIES

20. **Plaintiff Kyle McDaniel** is an individual domiciled in Cordova, Tennessee. Plaintiff Kyle McDaniel is a victim of the Data Breach and received a Notice of Data Breach Letter from TGCS.

21. **Plaintiff Rikki McDaniel** is an individual domiciled in Cordova, Tennessee. Plaintiff Rikki McDaniel is a victim of the Data Breach and received a Notice of Data Breach Letter from TGCS.

22. **Plaintiff Jon Williams** is an individual domiciled in Wilmington, North Carolina. Plaintiff Jon Williams is a victim of the Data Breach and received a Notice of Data Breach Letter from TGCS.

23. **Plaintiff Mojdeh Williams** is an individual domiciled in Wilmington, North Carolina. Plaintiff Mojdeh Williams is a victim of the Data Breach and received a Notice of Data Breach Letter from TGCS.

24. **Plaintiff Tom Simmons** is an individual domiciled in Durham, North Carolina. Plaintiff Tom Simmons is a victim of the Data Breach and received a Notice of Data Breach Letter from TGCS.

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

III. JURISDICTION AND VENUE

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

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

28. Defendant has sufficient minimum contacts in California and has intentionally availed itself 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. TGCS is a global market share leader in retail store technology.[8] There are over 2,000 employees working for TGCS serving over 120 countries

[8] TOSHIBA, https://commerce.toshiba.com/wps/portal/marketing/?urile=wcm:path:/en-us/home.

worldwide.[9]

21. According to Toshiba's latest financial reports the company's current revenue (TTM) is $23.53 Billion USD.[10]

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

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

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

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

26. Defendant recognized this duty and made the following claims on its website regarding its protection of sensitive data:

[9] *About Us*, TOSHIBA, https://commerce.toshiba.com/wps/portal/marketing/?urile=wcm:path:/en-us/home/company/about-us.

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

TGCS:

> Toshiba has implemented technical and organizational security measures to guarantee the security of your Personal Information. Users' Personal Information is stored in our secure networks and access is restricted to those employees and partners who are entitled to access our systems.[11]

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

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

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

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

31. Despite knowledge of their duties to keep Plaintiffs' and Class Members' PII secure, Toshiba failed to adequately protect its email accounts from

[11] *Privacy Policy*, TOSHIBA, https://commerce.toshiba.com/?urile=wcm:path:/en-us/common-content/general-content/privacy-policy&mapping=tgcs_new.portal.generaldetails.

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

B. Toshiba's Massive and Preventable Data Breach.

32. On an undisclosed date, Toshiba discovered suspicious activity within its email environment.[12]

33. After detecting the Breach, Toshiba claims it initiated an investigation in which it determined cybercriminals infiltrated Toshiba's email environment between December 4, 2023, and March 18, 2024.[13]

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

35. Toshiba claims the investigation of the Data Breach is still ongoing, but on May 14, 2024, it learned that personal information was potentially viewed by an unauthorized individual.[14]

36. The Private Information accessed without authorization in the Data Breach included highly sensitive information such as Social Security numbers and names—which can immediately be used to commit fraud and identity theft.[15]

37. Despite the Data Breach beginning in December 2023, Toshiba did not

---

[12] OFFICE OF THE MAINE ATTORNEY GENERAL, *Toshiba Global Commerce Solutions*, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/8fea1aeb-d918-4c0d-b40d-97990f1eb395.html.

[13] *Id.*

[14] *Id.*

[15] *Id.*

begin notifying individuals of the Data Breach until May 28, 2024,[16] with some not being notified until July 2024 or November 2024.

38. Omitted from the Notice of Data Breach Letters were the details of the root cause of the Data Breach, the vulnerabilities exploited, when the Data Breach began and ended, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

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

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

41. As the Data Breach and its timeline evidences, Toshiba did not use reasonable security measures appropriate to the nature of the sensitive Private

[16] *Id.*

Information collected from Plaintiffs and Class Members and maintained on Toshiba's emails, such as encrypting the information, deleting the data from Toshiba's emails accounts when it was no longer needed, requiring sufficient verification such as multi-factor authentication for email accounts, training employees about cybersecurity, phishing, and attempts to gain unauthorized access, investigating and addressing vulnerabilities in its data security practices, and/or implementing the necessary safeguards to enable Toshiba to identify malicious activity and curtail it when it happens. These failures allowed and caused cybercriminals to target Toshiba's email accounts and carry out the Data Breach.

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

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

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

45. In recognition of the severity of the Data Breach, and the imminent risk of harm Plaintiffs and the Class face, Toshiba made an offering of twenty-four

(24) months of identity theft protection services.[17] Such an offering is inadequate and will not prevent identity theft but will only alert Data Breach victims once identity theft has ***already occurred***.

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

47. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

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

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

49. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[18]

50. For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal

---

[17] *Id.*

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

government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[19] These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and the Class Members.

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

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[20]
> (Emphasis added).

52. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[21]

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

---

[19] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security 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/.

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

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

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

54. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[22]

55. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[23]

56. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[24]

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

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

---

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

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

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

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

58. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, a criminal can (i) obtain credit cards or loans; (ii) open a new bank account; (iii) empty existing bank accounts; (iv) get a fraudulent driver's license; (v) receive medical care; (vi) open a phone account; (vii) commit crimes that will show up on the victim's record; (viii) steal benefits and Social Security checks; (ix) set up utilities; and file a fraudulent tax returns.[26]

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

60. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[27]

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

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

[26] https://www.aura.com/learn/what-can-someone-do-with-your-social-security-number.

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

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

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

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

66. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank

---

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

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

[30] *Id.*

accounts and credit reports for unauthorized activity for years to come.

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

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

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property including PII;

c. Improper disclosure of their PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their PII;

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

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

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

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

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

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

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

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

71. Defendant acknowledged the harm caused by the Data Breach because it offered Plaintiffs and Class Members woefully inadequate identity theft repair and monitoring services. Twenty-four (24) months of identity theft and repair and monitoring is, however, inadequate to protect Plaintiffs and Class Members from a lifetime of identity theft risk.

72. Defendant further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur,

stating, "[w]e regret any inconvenience or concern this incident may have caused you."

73. Additionally, the Notice of Data Breach Letter sent to Plaintiffs and other Class Members recognized that Toshiba needed to improve its cybersecurity protocols, stating "[t]o help prevent a similar incident from occurring in the future, we implemented additional measures to enhance the security of our email environment."

74. These enhanced protections should have been in place before the Data Breach.

75. At Toshiba's suggestion, Plaintiffs are desperately trying to mitigate the damage that Toshiba has caused them.

76. Given the kind of Private Information Toshiba made accessible to hackers, however, Plaintiffs are certain to incur additional damages. Because identity thieves have their PII, Plaintiffs and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[31]

77. None of this should have happened because the Data Breach was entirely preventable.

---

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

D. Defendant was Aware of the Risk of Cyberattacks.

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

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

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

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

82. Cyberattacks against institutions such as Toshiba are targeted and frequent. According to the Identity Theft Resource Center's report covering the year 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that

involved sensitive information (Ex: Social Security numbers) increased slightly compared to 2020 (83 percent vs. 80 percent).” As stated in IBM’s 2022 report, “[f]or 83% of companies, it’s not if a data breach will happen, but when.”

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

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

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

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

87. Businesses operating in the technology sector, such as Toshiba, are a "wealth of sensitive data," and are "prime targets for hackers seeking financial gain, intellectual property theft, or simply to wreak havoc."[32]

88. Toshiba knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for it.

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

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

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

[32] https://www.offsec.com/blog/top-technology-sector-breaches-and-threats/.

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

E. Toshiba Could Have Prevented the Data Breach.

93. Data breaches are preventable.[33] 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."[34] 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 . . . ."[35]

94. "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*."[36]

---

[33] 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.

[34] *Id.* at 17.

[35] *Id.* at 28.

[36] *Id.*

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

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

97. 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.[37]

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

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

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

---

[37] *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.

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

102. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[38]

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

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

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

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[39]

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

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as

[39] *Id.* at 3–4.

those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) ….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[40]

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

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

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

- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[41]

106. 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

[41] *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/.

happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.

- **Keep Your Security Up to Date:** Always install the latest patches and updates. Look for additional means of protection, like email authentication and intrusion prevention software, and set them to update automatically on your computers. On mobile devices, you may have to do it manually.
- **Alert Your Staff:** Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.
- **Deploy a Safety Net:** Use email authentication technology to help prevent phishing emails from reaching your company's inboxes in the first place.[42]

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

108. Given that Defendant was storing the PII of thousands of individuals, Defendant could have and should have implemented all the above measures to prevent and detect cyber intrusions.

[42]https://www.ftc.gov/system/files/attachments/phishing/cybersecurity_sb_phishing.pdf.

109. Specifically, among other failures, Toshiba had far too much confidential unencrypted information held on its email systems. Such PII should have been segregated into an encrypted system.[43]

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

111. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, saying simply: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[44] Toshiba, rather than following this basic standard of care, kept thousands of individuals' unencrypted PII indefinitely.

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

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

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

[44] *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, at p. 6.

F. Plaintiffs' Individual Experiences

Plaintiff Kyle McDaniel

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

115. Plaintiff Kyle McDaniel is a former employee of Toshiba.

116. Defendant was in possession of Plaintiff Kyle McDaniel's Private Information before, during, and after the Data Breach.

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

118. As a result of the Data Breach, Plaintiff Kyle McDaniel has already expended over **100 hours** of his time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach. This includes: (i) investigating the Data Breach; (ii) investigating how best to ensure that he is protected from identity theft; (iii)

reviewing his account statements, credit reports, and/or other information; and (iv) mitigating the fraud and identity theft he has already experienced.

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

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

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

122. Plaintiff Kyle McDaniel has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of

future harm Plaintiff Kyle McDaniel, and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Kyle McDaniel and the Class.

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

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

125. Plaintiff Kyle McDaniel has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Kyle McDaniel should have received from Defendant and Defendant's defective and deficient performance of that

obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Rikki McDaniel

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

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

128. Defendant was in possession of Plaintiff Rikki McDaniel's Private Information before, during, and after the Data Breach.

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

130. As a result of the Data Breach, Plaintiff Rikki McDaniel has already expended over **100 hours** of her time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach. This includes: (i) investigating the Data Breach; (ii) investigating how best to ensure that she is protected from identity theft; and (iii) reviewing her account statements, credit reports, and/or other information.

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

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

133. Knowing that thieves intentionally targeted and stole her Private Information, including her Social Security number, and knowing that her Private Information is in the hands of cybercriminals has caused Plaintiff Rikki McDaniel great anxiety beyond mere worry. Specifically, Plaintiff Rikki McDaniel has lost

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

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

135. Plaintiff Rikki McDaniel has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Rikki McDaniel should have received from Defendant and Defendant's 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 Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Jon Williams

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

137. Plaintiff Jon Williams is a former employee of Toshiba.

138. Defendant was in possession of Plaintiff Jon Williams' Private Information before, during, and after the Data Breach.

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

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

141. Plaintiff Jon Williams places significant value on the security of his Private Information and does not readily disclose it. Plaintiff Jon Williams has

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

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

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

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

145. Plaintiff Jon Williams has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and

identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Jon Williams should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Mojdeh Williams

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

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

148. Defendant was in possession of Plaintiff Mojdeh Williams' Private Information before, during, and after the Data Breach.

149. Because of the Data Breach, there is no doubt Plaintiff Mojdeh Williams' highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from TGCS disclosed that an

unauthorized third-party accessed Defendant's system. The *modus operandi* of cybercriminals involves stealing Private Information for financial gain. Cybercriminals may use stolen identities to conceal their own true identity or carry out a range of fraudulent activities, from credit card fraud to impersonation. As such, Plaintiff Mojdeh Williams and the Class are at imminent risk of identity theft and fraud.

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

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

152. Plaintiff Mojdeh Williams places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Mojdeh Williams has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

153. Plaintiff Mojdeh Williams has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative,

given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the present and increased risk of future harm Plaintiff Mojdeh Williams, and the Class now face by offering temporary, non-automatic credit monitoring services to Plaintiff Mojdeh Williams and the Class.

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

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

156. Plaintiff Mojdeh Williams has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of her valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by her Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of her Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the

benefit of the bargain with Defendant to provide adequate and reasonable data security—i.e., the difference in value between what Plaintiff Mojdeh Williams should have received from Defendant and Defendant's 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 Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Tom Simmons

157. Plaintiff Tom Simmons received a Notice of Data Breach Letter from TGCS informing him that his highly confidential Private Information was compromised in the Data Breach.

158. Plaintiff Tom Simmons is a former employee of Toshiba.

159. Defendant was in possession of Plaintiff Tom Simmons's Private Information before, during, and after the Data Breach.

160. Because of the Data Breach, there is no doubt Plaintiff Tom Simmons's highly confidential Private Information is in the hands of cybercriminals. Reason being, the Notice of Data Breach Letter from TGCS disclosed that an unauthorized third-party accessed Defendant's system. The *modus operandi* of cybercriminals involves stealing Private Information for financial gain. Cybercriminals may use stolen identities to conceal their own true identity or carry out a range of fraudulent activities, from credit card fraud to impersonation. As

such, Plaintiff Tom Simmons and the Class are at imminent risk of identity theft and fraud.

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

162. Plaintiff Tom Simmons places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Tom Simmons has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

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

164. Knowing that thieves intentionally targeted and stole his Private Information, including his Social Security number, and knowing that his Private Information is in the hands of cybercriminals has caused Plaintiff Tom Simmons great anxiety beyond mere worry. Specifically, Plaintiff Tom Simmons has lost

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

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

166. Plaintiff Tom Simmons has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Tom Simmons should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

V. CLASS ACTION ALLEGATIONS

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

168. 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.**

169. Excluded from the Class are Defendant, any entity in which Defendant have a controlling interest, and Defendant's 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.

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

171. Plaintiffs anticipate the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

172. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

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

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

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

176. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Toshiba's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device

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

177. **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 Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's PII;

c. Whether Defendant 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;

j. Whether Toshiba breached implied contractual duties to Plaintiffs and the Class to use reasonable care in protecting their PII;

k. Whether Toshiba failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and the Class;

l. Whether Toshiba continues to breach duties to Plaintiffs and the Class;

m. Whether Plaintiffs and the Class suffered injury as a proximate result of Toshiba's negligent actions or failures to act;

n. Whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Toshiba's actions alleged herein constitute gross negligence, and whether Plaintiffs and Class Members are entitled to punitive damages.

I. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

178. Plaintiffs incorporate paragraphs 1–177 as though fully set forth herein.

179. Toshiba solicited, gathered, and stored the PII of Plaintiffs and Class Members.

180. Upon accepting and storing the PII of Plaintiffs and Class members on

its computer systems and networks, Defendant undertook and owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

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

182. Because of this special relationship, Defendant required Plaintiffs and Class members to provide their PII, including names, Social Security numbers, and other PII.

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

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

185. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiffs' and Class members' PII from being foreseeably accessed, and its improper retention of PII it

was not required to maintain, Defendant negligently failed to observe and perform its duty.

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

187. Defendant knew cybercriminals routinely target large corporations through cyberattacks to steal customer and employee PII. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

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

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

190. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense

precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs, and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's email accounts, networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class members' PII in its possession by using reasonable and adequate security procedures and systems;

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

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

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

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

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

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

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

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

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

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

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

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

196. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class

members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class members while it was within Defendant's possession and control.

197. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class members, Defendant prevented Plaintiffs and Class members from taking meaningful, proactive steps to securing its PII and mitigating damages.

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

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

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

201. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiffs and Class members have suffered, as Plaintiffs have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PII is used; (ii) the publication and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) lost opportunity

costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of employees in their continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII for the rest of their lives. Thus, Plaintiffs and the Class are entitled to damages in an amount to be proven at trial.

202. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

203. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

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

204. Plaintiffs incorporates paragraphs 1–177 as though fully set forth herein.

205. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant 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.

206. 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 Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

207. Defendant gathered and stored the PII of Plaintiffs and the Class as part of Defendant's business which affects commerce.

208. Defendant 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.

209. Defendant breached its 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.

210. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

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

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

213. Defendant breached its duties to Plaintiffs and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class's PII.

214. Defendant breached its duties to Plaintiffs and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiffs and the Class.

215. Defendant's violations of the FTC Act constitute negligence *per se*.

216. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

217. The injury and harm that Plaintiffs and Class members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

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

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

219. Plaintiffs incorporate paragraphs 1–177 as though fully set forth herein.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

235. As a result of Toshiba's failures to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive the full benefit of their bargains with Toshiba and instead received services of a diminished value compared to that described in the implied contracts. Plaintiffs and Class Members were therefore damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and that which they received.

236. Had Toshiba disclosed that its data security procedures were inadequate or that it did not adhere to industry-standard for cybersecurity, neither Plaintiffs, Class Members, nor any reasonable person would have contracted with Toshiba.

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

238. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Toshiba.

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

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

240. Plaintiffs incorporate paragraphs 1–177 as though fully set forth herein.

241. Plaintiffs allege this claim in the alternative to his breach of implied contract claim.

242. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiffs' retained data and commercialized and used Plaintiffs' and Class Members' PII for business purposes.

243. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

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

245. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members

for the value that their PII provided.

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

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

248. Plaintiffs and Class Members have no adequate remedy at law.

249. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

250. As a direct and proximate result of Defendant's conduct, Plaintiffs and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required

Plaintiffs' efforts to prevent from succeeding.

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

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

252. Plaintiffs incorporate paragraphs 1–177 as though fully set forth herein.

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

254. As previously alleged, Plaintiffs and members of the Class are entered into implied contracts with Defendant, which contracts require Defendant to provide adequate security for the PII collected from Plaintiffs and the Class.

255. Defendant owed and still owes a duty of care to Plaintiffs and Class members that require it to adequately secure Plaintiffs' and Class members' PII.

256. Upon reason and belief, Defendant still possesses the PII of Plaintiffs and the Class members.

257. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class members.

258. Since the Data Breach, Defendant have not yet announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities

in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

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

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

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

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

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering

Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

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

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

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

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

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

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

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

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

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

II. DEMAND FOR JURY TRIAL

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

Dated: April 17, 2025

By: */s/ Andrew G. Gunem*

Andrew G. Gunem (SBN 354042)
Raina C. Borrelli (*pro hac vice*)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com
raina@straussborrelli.com

William B. Federman (*pro hac vice*)
Kennedy M. Brian (*pro hac vice*)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com
E: kpb@federmanlaw.com

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

Attorneys for Plaintiffs and the Proposed Class