

BRONSTER FUJICHAKU ROBBINS  
A Law Corporation

MARGERY S. BRONSTER #4750  
ROBERT M. HATCH #7724  
NOELLE E. CHAN #11280  
1003 Bishop Street, Suite 2300  
Honolulu, Hawai'i 96813  
Telephone: (808) 524-5644  
Facsimile: (808) 599-1881  
Email: [mbronster@bfrhawaii.com](mailto:mbronster@bfrhawaii.com)  
[rhatch@bfrhawaii.com](mailto:rhatch@bfrhawaii.com)

**Electronically Filed**  
**FIRST CIRCUIT**  
**1CCV-23-0000553**  
**28-APR-2023**  
**03:23 PM**  
**Dkt. 1 CMPS**

CAFFERTY CLOBES MERIWETHER &  
SPRENGEL LLP  
DANIEL O, HERRERA (*pro hac vice* to be submitted)  
NICKOLAS J. HAGMAN (*pro hac vice* to be submitted)  
135 S. LaSalle, Suite 3210  
Chicago, Illinois 60603  
Telephone: (312) 782-4880  
Facsimile: (312) 782-4485  
Email: [dherrera@caffertyclobes.com](mailto:dherrera@caffertyclobes.com)  
[rnhagman@caffertyclobes.com](mailto:rnhagman@caffertyclobes.com)

Attorneys for Plaintiff TONY LEE  
and the Proposed Class

**IN THE CIRCUIT COURT OF THE FIRST CIRCUIT**

**STATE OF HAWAI'I**

TONY LEE, individually, and on behalf of all  
others similarly situated,

Plaintiff,

v.

HAWAIIUSA FEDERAL CREDIT UNION,

Defendant.

Case No. \_\_\_\_\_

**CLASS ACTION COMPLAINT;  
EXHIBIT "A"; DEMAND FOR JURY  
TRIAL; SUMMONS**

## **CLASS ACTION COMPLAINT**

Plaintiff Tony Lee (“Plaintiff”), individually, and on behalf of all others similarly situated, brings this action against HawaiiUSA Federal Credit Union (“HawaiiUSA” or “Defendant”), by and through his attorneys, and alleges, based upon personal knowledge as to his own actions, and based upon information and belief as to all other matters, as follows.

### **I. INTRODUCTION**

1. Defendant is a full-service financial institution providing a wide range of banking and loan services to individuals in Hawai‘i, including mortgages, lines of credit, personal loans, auto loans, credit cards, online and mobile banking, checking and savings accounts, and other branch services.<sup>1</sup>

2. In order to provide these services, Defendant collects, maintains, and stores both its employees’ and customers’ highly sensitive personal and financial information, including, but not limited to: names, Social Security numbers, financial account numbers, credit and debit card numbers, and consumer account information including security codes, access codes, passwords, or PINs (“personally identifying information” or “PII”).<sup>2</sup> Defendant’s employees and customers provide this information under the expectation that Defendant, a sophisticated financial services provider, will safeguard their highly valuable PII.

3. Defendant, however, failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive PII of approximately 20,889 individuals, including the

---

<sup>1</sup> *Services*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/Banking/Personal/Services> (last accessed Apr. 25, 2023).

<sup>2</sup> *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed Apr. 25, 2023); *See HawaiiUSA Federal Credit Union confirms Recent Data Breach Affected Over 20k Customers*, JD Supra, <https://www.jdsupra.com/legalnews/hawaiiusa-federal-credit-union-confirms-6926519/> (last accessed Apr. 25, 2023).

Plaintiff and Class members.<sup>3</sup> As a direct, proximate, and foreseeable result of Defendant's inexcusable failure to implement reasonable security protections sufficient to prevent an eminently avoidable cyberattack, unauthorized actors compromised Defendant's network and accessed thousands of consumer files containing highly-sensitive PII.<sup>4</sup>

4. Specifically, on or around December 12, 2022, Defendant's current and former employees' and consumers' sensitive personal and/or financial data was compromised when unauthorized actors were able to breach an employee's email account on Defendant's network and access files containing PII for approximately 20,889 individuals (the "Data Breach").<sup>5</sup>

5. Despite the fact that many of the categories of PII exposed in the Data Breach, such as Social Security numbers, cannot be changed, Defendant failed to detect the breach until on or around March 15, 2023—more than *three* months after the breach occurred—and failed to notify affected individuals until on or around April 5, 2023, almost *four* months after unauthorized individuals accessed Plaintiff's and current and former employees' and consumers' highly sensitive PII that is stored on Defendant's systems.<sup>6</sup>

6. Defendant's failure to promptly notify Plaintiff and Class members that their PII was exfiltrated due to Defendant's security failures virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse and/or disseminate that PII

---

<sup>3</sup> *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed Apr. 25, 2023).

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

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

<sup>6</sup> *See Exhibit A; Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed Apr. 25, 2023); *HawaiiUSA Federal Credit Union*, Office of the Maine Attorney General, [file:///ph1Inas4/OLawless179\\$/Personal/Downloads/HawaiiUSA%20-%20Maine%20Attachment%20\(2\).pdf](file:///ph1Inas4/OLawless179$/Personal/Downloads/HawaiiUSA%20-%20Maine%20Attachment%20(2).pdf) (last accessed Apr. 25, 2023).

before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

7. Defendant failed to take sufficient and reasonable measures to safeguard its data security systems and protect highly sensitive data in order to prevent the Data Breach from occurring; to disclose to current and former employees and consumers, and the public at large, the material fact that it lacked appropriate data systems and security practices to secure PII and financial information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to Defendant's failures, Plaintiff and approximately 20,889 individuals suffered substantial harm and injury.

8. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and Class members' PII was accessed and acquired by unauthorized third-parties for the express purpose of misusing the data and causing further irreparable harm to the personal, financial, reputational, and future well-being of Defendant's current and former employees and consumers. Plaintiff and Class members face the real, immediate, and likely danger of identity theft and misuse of their PII, especially because their PII was specifically targeted by malevolent actors.

9. Plaintiff and Class members suffered injuries as a result of Defendant's conduct including, but not limited to: lost or diminished value of their PII; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; time needed to change

usernames and passwords on their accounts; time needed to investigate, correct and resolve unauthorized access to their accounts; time needed to deal with spam messages and e-mails received subsequent to the Data Breach; charges and fees associated with fraudulent charges on their accounts; and the continued and increased risk of compromise 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 their PII. These risks will remain for the lifetimes of Plaintiff and the Class.

10. Accordingly, Plaintiff brings this action on behalf of all those similarly situated to seek relief from Defendant's failure to reasonably safeguard Plaintiff's and Class members' PII; its failure to reasonably provide timely notification that Plaintiff's and Class members' PII had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their PII.

## II. PARTIES

### Plaintiff Tony Lee

11. Plaintiff Tony Lee is a resident and citizen of Hawai'i, residing in Mililani, Hawai'i.

12. Plaintiff received Defendant's Notice of Data Breach (the "Notice") sometime after April 5, 2023.

13. Plaintiff is currently, and has been for over ten years, a customer of Defendant. Specifically, Plaintiff has maintained both a savings and checking account with Defendant, opened a debit card and credit card, taken personal loans, and linked his banking accounts to his PayPal.

14. In the Notice that Plaintiff received sometime after April 5, 2023 (attached hereto as **Exhibit A**), Defendant informed Plaintiff that an unauthorized third-party had gained access to an employee's email account, and an internal investigation revealed that an email or attachment

thereto present in the employee's inbox contained Plaintiffs' PII, including his Social Security number, credit and debit card number, bank and financial account number and other financial information. Defendant advised Plaintiff to, among other things, access and review his credit reports and consider placing a freeze on his credit account.

**Defendant HawaiiUSA Federal Credit Union**

15. Defendant HawaiiUSA Federal Credit Union is a financial and banking services corporation organized under the laws of Hawai'i with its principal place of business at 1226 College Walk, Honolulu, Hawai'i 96817.<sup>7</sup> Defendant operates more than a dozen branches, all of which are located in the Hawaiian Islands.

**III. JURISDICTION AND VENUE**

16. This Court has jurisdiction over this action pursuant to Hawai'i Revised Statutes ("HRS") § 603-21.5. HawaiiUSA Federal Credit Union purposefully availed itself of the laws, protections, and advantages of doing business in Hawai'i, and the events and transactions giving rise to the cause of action alleged herein occurred in Hawai'i.

17. Venue is proper under HRS § 603-36 because HawaiiUSA Federal Credit Union is domiciled in, resides in, and conducts business in the County of Honolulu and the State of Hawai'i.

**IV. FACTUAL ALLEGATIONS**

**A. Defendant – Background**

18. Defendant is a full-service financial corporation that provides a variety of banking and loan services including checking and savings accounts, mobile and online banking, direct

---

<sup>7</sup> *HawaiiUSA Federal Credit Union*, Hawaii.gov, <https://hbe.ehawaii.gov/documents/trade.html?fileNumber=485760ZZ&certificate=4263242> (last accessed Apr. 25, 2023).

deposit, telephone banking, in-branch services, business checking and savings accounts, business protection, mortgages, auto loans, personal loans, lines of credit, home equity loans, credit cards, business loans, and various other financial services.<sup>8</sup> Defendant represents that consumers can “[e]njoy secure and convenient online banking, or bank by appointment at any of our Oahu, Maui, Big Island, or Kauai branches.”<sup>9</sup>

19. As part of its financial and business operations, Defendant requires that employees and consumers provide their PII and financial information. Defendant collects, maintains, and stores highly sensitive PII, including but not limited to: full names, Social Security numbers, financial account numbers, credit and debit card numbers, and consumer account information including security codes, access codes, passwords, or PINs.

20. On information and belief, at the time of the Data Breach, Defendant had failed to implement necessary data security safeguards, which resulted in unauthorized third parties accessing the PII of approximately 20,889 current and former employees and consumers.<sup>10</sup>

21. Current and former employees and customers of Defendant, such as Plaintiff and the Class, made their PII available to Defendant with the reasonable expectation that Defendant would comply with its obligation to keep that sensitive and personal information confidential and secure from illegal and unauthorized access, and that Defendant would provide them with prompt and accurate notice of any unauthorized access to their PII.

---

<sup>8</sup> *Bank*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/Banking> (last accessed Apr. 25, 2023); *Borrow*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/Loans> (last accessed Apr. 25, 2023).

<sup>9</sup> *HawaiiUSA Federal Credit Union*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/> (last accessed Apr. 25, 2023).

<sup>10</sup> *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed Apr. 25, 2023).

22. Unfortunately for Plaintiff and Class members, Defendant failed to carry out its duty to safeguard sensitive PII and provide adequate data security, thus failing to protect Plaintiff and Class members from having their PII exfiltrated during the Data Breach.

**B. The Data Breach**

23. Defendant disclosed in a Notice sent on or about April 5, 2023, to Plaintiff and other affected individuals that there was “an incident involving unauthorized access to an employee’s email account” ... “for a short period of time on December 12, 2022. *See* Notice of Data Breach, attached hereto as Exhibit A. Further, Defendant acknowledged that the unauthorized party was able to exfiltrate Plaintiff’s and Class members’ PII. *See* Exhibit A.

24. Defendant further admitted that despite a “careful review of the contents of the accounts”, Defendant did not determine the breadth of the unauthorized access until on or after March 15, 2023. *See* Exhibit A.

25. Defendant failed to disclose to Plaintiff and other victims of the Data Breach when the unauthorized third party first gained access to Defendant’s systems and how long the unauthorized actor had access to Plaintiff’s and Class members’ information.

26. Defendant asserts that upon discovering the Data Breach, “a cybersecurity firm was engaged, and an investigation was conducted.” *See* Exhibit A. However, Defendant was unable to secure its computer systems until on or after March 15, 2023, when it first discovered the extent of the Data Breach and more than *three* months after the Data Breach occurred. Defendant failed to disclose to Plaintiff and Class members that Defendant was unable to quickly remove the hacker’s access to Defendant’s computer systems.

27. Despite discovering the Data Breach on March 15, 2023, and confirming that the unauthorized actor may have accessed and exfiltrated employees’ and consumers’ PII, including



Social Security numbers and financial account information, Defendant delayed sending individualized notice to affected individuals until on or after April 5, 2023. *See* Exhibit A.

28. During the time that the unauthorized individuals had access to Defendant's network, they were able to access, view and potentially acquire personal, sensitive, and protected PII belonging to over 20,889 current and former employees and customers of Defendant.

**C. Defendant's Many Failures Both Prior to and Following the Breach**

29. Defendant could have prevented this Data Breach by engaging in proper data security practices, including properly encrypting or otherwise protecting its equipment and network files containing PII, and permanently deleting sensitive data and PII when it is no longer necessary to store such data.

30. To be sure, collecting, maintaining, and protecting PII is vital to virtually every aspect of Defendant's operations as a financial institution. Yet, Defendant failed to detect that its own data system had been compromised until sometime around March 15, 2023.<sup>11</sup>

31. When Defendant finally acknowledged that it had experienced a breach, it failed to fully inform affected individuals of the length of time that the unauthorized actors had access to Plaintiff's and Class members' PII, or even the full extent of the PII that was accessed during the Data Breach.

32. Defendant's failure to properly safeguard Plaintiff's and Class members' PII allowed the unauthorized actors to access this highly valuable information, and Defendant's failure to timely notify Plaintiff and other victims of the Data Breach that their PII was accessed served only to exacerbate the harms they suffered as a direct and proximate result thereof because it

---

<sup>11</sup> *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed Apr. 25, 2023).

precluded them from taking meaningful steps to safeguard their identities prior to the further dissemination and misuse of their PII.

33. The Data Breach also highlights the inadequacies inherent in Defendant's network monitoring procedures. If Defendant had properly monitored its cyber security systems, it would have prevented the Data Breach, discovered the Data Breach sooner, and/or have prevented the hackers from accessing and/or exfiltrating PII and financial information.

34. First, Defendant failed to timely discover the Data Breach and immediately secure its computer systems to protect its current and former employees' and consumers' PII and financial information. It instead allowed unauthorized actors to continue to have access to its computer systems for over *three* months—until Defendant finally discovered the Data Breach in March 2023.<sup>12</sup>

35. Second, Defendant failed to timely notify affected individuals, including Plaintiff and Class members, that their highly sensitive PII had been accessed by unauthorized third parties. Defendant waited approximately *four* months after the Data Breach occurred to notify victims of the Data Breach that their PII had been compromised.

36. Third, Defendant made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. Although the notice offered victims a complimentary one-year membership to Experian's IdentityWorks credit monitoring service, Plaintiff's and Class members' PII, including their Social Security numbers, cannot be changed and will remain at risk long beyond one year. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

---

<sup>12</sup> *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed Apr. 25, 2023).

37. Further, Defendant likely failed to adequately protect current and former employees' and consumers' PII by storing the data on its network systems far beyond the amount of time necessary to maintain such information. The failure to permanently delete or purge sensitive and personal information once it is no longer necessary to store such information creates an unnecessary and unreasonable risk of identity theft for current and former employees' and consumers.

38. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and notify Plaintiff and Class members with reasonable timeliness that their personal and financial information had been accessed and/or exfiltrated due to Defendant's security failures, allowed unauthorized individuals to access, misappropriate and/or misuse Plaintiff's and Class members' PII for almost *four* months before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

#### **D. Data Breaches Pose Significant Threats**

39. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

40. In 2022, the Identity Theft Resource Center's Annual End-of-Year Data Breach Report listed 1,802 total data compromises involving 422,143,312 victims for 2022, which was just 50 data compromises short of the current record set in 2021.<sup>13</sup>

---

<sup>13</sup> *2022 End of Year Data Breach Report*, Identity Theft Resource Center (January 25, 2023), available at: [https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm\\_source=press+release&utm\\_medium=web&utm\\_campaign=2022+Data+Breach+Report](https://www.idtheftcenter.org/publication/2022-data-breach-report/?utm_source=press+release&utm_medium=web&utm_campaign=2022+Data+Breach+Report) .

41. Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, confirms that the number of data breaches has been steadily increasing since it began a survey of data compromises in 2005 with 157 compromises reported that year, to a peak of 1,862 in 2021, to 2022's total of 1,802.<sup>14</sup> The number of impacted individuals has also risen precipitously from approximately 318 million in 2015 to 422 million in 2022, which is an increase of nearly fifty percent.<sup>15</sup>

42. Data breaches are a constant threat because PII is routinely traded on the dark web as a simple commodity, with Social Security numbers being sold at as little as \$2.99 apiece and passports retailing for as little as \$15 apiece.<sup>16</sup>

43. In addition, the severity of the consequences of a compromised Social Security number belies the ubiquity of stolen numbers on the dark web. Criminals and other unsavory enterprises can fraudulently take out loans under the victims' name, open new lines of credit, and cause other serious financial difficulties for victims:

“[a] dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.”<sup>17</sup>

---

<sup>14</sup> *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2022*, Statista (January 2023), available at: <https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed>.

<sup>15</sup> *Id.*

<sup>16</sup> *What is your identity worth on the dark web?* Cybernews (September 28, 2021), available at: <https://cybernews.com/security/whats-your-identity-worth-on-dark-web>.

<sup>17</sup> United States Social Security Administration, *Identity Theft and Your Social Security Number*, United States Social Security Administration (July 2021), available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

This is exacerbated by the fact that the problems arising from a compromised Social Security number are exceedingly difficult to resolve. A victim is forbidden from proactively changing his or her number unless and until it is actually misused and harm has already occurred. And even this delayed remedial action is unlikely to undo the damage already done to the victims:

“Keep in mind that a new number probably won’t solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won’t guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.”<sup>18</sup>

44. In light of the dozens of high-profile financial information data breaches that have been reported in recent years, entities like Defendant charged with maintaining and securing consumer PII know the importance of protecting that information from unauthorized disclosure. Indeed, on information and belief, Defendant was aware of highly publicized security breaches where PII and protected financial information was accessed by unauthorized cybercriminals.

45. In addition, the Federal Trade Commission (“FTC”) has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers’ personal data. The FTC publicized these enforcement actions to place companies like Defendant on notice of their obligation to safeguard consumer information.

46. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

---

<sup>18</sup> *Id.*

47. Given the nature of Defendant's Data Breach, as well as the length of the time Defendant's networks were breached and the long delay in notification to the Class, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class members' PII can easily obtain Plaintiff's and Class members' tax returns or open fraudulent credit card accounts in their names.

48. Based on the foregoing, the Social Security numbers compromised in the Data Breach hold significant value on the dark web.<sup>19</sup> The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

49. To date, Defendant has offered its consumers *only one year* of identity theft monitoring services. The offered services are inadequate to protect Plaintiff and the Class from the threats they will face for years to come, particularly in light of the PII at issue here.

50. Despite the prevalence of public announcements of data breach and data security compromises, its own acknowledgment of the risks posed by data breaches, and its own acknowledgment of its duties to keep PII private and secure, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the Class from misappropriation. As a result, the injuries to Plaintiff and the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for its current and former employees and consumers.

**E. Defendant Had a Duty and Obligation to Protect PII**

51. Defendant has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and Class members' PII.

---

<sup>19</sup> See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, Forbes (Mar 25, 2020), available at <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

Defendant's obligations are derived from: 1) government regulations and state laws, including FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII and financial records. Plaintiff and Class members provided, and Defendant obtained, their PII on the understanding that their PII would be protected and safeguarded from unauthorized access or disclosure.

52. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>20</sup> The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."<sup>21</sup>

53. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.<sup>22</sup>

54. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.<sup>23</sup> The guidelines note businesses should protect the personal information

---

<sup>20</sup> 17 C.F.R. § 248.201 (2013).

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

<sup>22</sup> *Start With Security*, Federal Trade Commission (June 2015), available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

<sup>23</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Comm'n

that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.<sup>24</sup> The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.<sup>25</sup> Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, the fact that the Breach went undetected, and the amount of data exfiltrated.

55. Here, at all relevant times, Defendant was fully aware of its obligation to protect the PII and protected financial information of its current and former employees and consumers, including Plaintiff and the Class, and on information and belief, Defendant is a sophisticated and technologically savvy financial services facility that relies extensively on technology systems and networks to maintain its practice, including storing its employees' and consumers' PII and financial information in order to operate its business.

56. Defendant had, and continues to have, a duty to exercise reasonable care in collecting, storing, and protecting PII from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and Plaintiff and Class members. Defendant alone had the exclusive ability to implement adequate security measures to its cyber security network to secure and protect Plaintiff's and Class members' PII.

---

(October 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

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

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



57. Defendant's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential data constitutes unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

58. Further, Defendant had a duty to promptly notify Plaintiff and the Class that their PII was accessed by unauthorized persons.

**F. Defendant Violated FTC and Industry Standard Data Protection Protocols**

59. The FTC rules, regulations, and guidelines obligate businesses to protect PII, from unauthorized access or disclosure by unauthorized persons.

60. At all relevant times, Defendant was fully aware of its obligation to protect the PII entrusted to it by both Plaintiff and the Class because it is a sophisticated business entity that is in the business of collecting and maintaining PII, including financial information.

61. Defendant was also aware of the significant consequences of its failure to protect PII for the thousands of employees and consumers who provided their PII and financial information to Defendant, and knew that this data, if hacked, would cause injuries to employees and consumers, including Plaintiff and Class members.

62. Unfortunately, Defendant failed to comply with FTC rules, regulations and guidelines, and industry standards concerning the protection and security of PII. As evidenced by the duration, scope, and nature of the Data Breach, among its many deficient practices, Defendant failed in, *inter alia*, the following respects:

- a. Developing and employing adequate intrusion detection systems;
- b. Engaging in regular reviews of audit logs and authentication records;
- c. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

- d. Ensuring the confidentiality and integrity of current and former employees' and consumers' PII, including protected financial information and records that Defendant receives and maintains;
- e. Protecting against any reasonably anticipated threats or hazards to the security or integrity of its current and former employees' and consumers' PII;
- f. Implementing policies and procedures to prevent, detect, contain, and correct security violations;
- g. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;
- h. Implementing technical policies, procedures and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access;
- i. Permanently deleting and purging from all systems confidential and sensitive information, such as PII and protected financial information, when it is no longer necessary to maintain the information; and
- j. Other similar measures to protect the security and confidentiality of its current and former employees' and consumers' PII.

63. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former employees and consumers of Defendant would have been notified sooner, allowing them to promptly take protective and mitigating actions.

**G. Defendant's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations**

64. Defendant purports to care about data security and safeguarding employees' and consumers' PII, and represents that it will keep secure and confidential the PII belonging to its current and former employees and consumers.

65. Plaintiff's and Class members' PII and financial information were provided to Defendant in reliance on its promises and self-imposed obligations to keep PII and financial information confidential, and to secure the PII and financial information from unauthorized access by malevolent actors. Defendant failed to do so.

66. The length of the Data Breach also demonstrates that Defendant failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors to periodically test its network, servers, systems and workstations.

67. Had Defendant undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendant would have detected the Data Breach prior to the hackers extracting data from Defendant's networks, and Defendant's current and former employees and consumers would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

68. Indeed, following the Data Breach, Defendant effectively conceded that its security practices were inadequate and ineffective because since discovering the Breach it has "taken steps to enhance [its] existing security measures." *See* Exhibit A.

#### **H. Plaintiff and the Class Suffered Harm Resulting from the Data Breach**

69. Like any data hack, the Data Breach presents major problems for all affected.<sup>26</sup>

70. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC

---

<sup>26</sup> Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at <https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers>.

notes, “once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance.”<sup>27</sup>

71. The ramifications of Defendant’s failure to properly secure the PII of Plaintiff and Class members, are severe. Identity theft occurs when someone uses another person’s financial, and personal information, such as that person’s name, address, Social Security number, and other information, without permission in order to commit fraud or other crimes.

72. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

73. Furthermore, PII has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

74. Accordingly, Defendant’s wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiff and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.<sup>28</sup> Indeed, “[t]he level of risk is growing for anyone whose information is stolen in a data breach.”<sup>29</sup> Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that “[t]he theft of SSNs places consumers

---

<sup>27</sup>*Warning Signs of Identity Theft*, Federal Trade Comm’n, available at <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft> (last accessed March 11, 2023).

<sup>28</sup> *Data Breach Victims More Likely To Suffer Identity Fraud*, INSURANCE INFORMATION INSTITUTE BLOG (February 23, 2012), available at <http://www.iii.org/insuranceindustryblog/?p=267>.

<sup>29</sup> Susan Ladika, *Study: Data Breaches Pose A Greater Risk*, CREDITCARDS.COM (July 23, 2014), available at <http://www.creditcards.com/credit-card-news/data-breach-id-theft-risk-increase-study-1282.php>.

at a substantial risk of fraud.”<sup>30</sup> Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that has not yet been exploited by cybercriminals presents a concrete risk that the cybercriminals who now possess Class members’ PII will do so at a later date or re-sell it.

75. In response to the Data Breach, Defendant offered to provide certain individuals whose PII was exposed in the Data Breach with one year of credit monitoring. However, one year of complimentary credit monitoring is a period much shorter than what is necessary to protect against the lifelong risk of harm imposed on Plaintiff and Class members by Defendant’s failures.

76. Moreover, the credit monitoring offered by Defendant is inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive PII.

77. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

- a. Theft of PII, including protected financial information;
- b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;
- c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;
- d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken

---

<sup>30</sup> THE CONSUMER DATA INSECURITY REPORT: EXAMINING THE DATA BREACH- IDENTITY FRAUD PARADIGM IN FOUR MAJOR METROPOLITAN AREAS, available at [https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport\\_byNCL.pdf](https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf) (last accessed March 11, 2023).

from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, if they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

- e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and
- f. The loss of Plaintiff's and Class members' privacy.

78. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII and protected financial information being accessed by cybercriminals, risks that will not abate within a mere one year: the unauthorized access of Plaintiff's and Class members' PII, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach. The one year of credit monitoring that Defendant offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class members have suffered and will continue to suffer as a result of the Data Breach.

79. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure PII and financial information, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

80. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose PII and financial information was accessed in the Data Breach.

81. Defendant is aware of the ongoing harm that the Data Breach has and will continue to impose on Defendant's current and former employees and consumers, as the notice that it sent to Plaintiff and Class members regarding the Data Breach advises victims that "it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months." *See* Exhibit A.

**I. Plaintiff Lee's Experience**

82. On or around April 5, 2023, Plaintiff Lee received a notice from Defendant that his PII had been improperly accessed and/or obtained by third parties. This notice indicated that Plaintiff Lee's PII was compromised in the Data Breach.

83. As a result of the Data Breach, Plaintiff Lee has made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to, researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff Lee has spent several hours dealing with the Data Breach, valuable time Plaintiff Lee otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

84. On information and belief, the PII unauthorized third parties have made available for purchase on the dark web was exfiltrated from Defendant during the Data Breach.

85. As a result of the Data Breach, Plaintiff Lee has suffered anxiety due to the public dissemination of his PII, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Lee is concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

86. Plaintiff Lee suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Lee; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

87. As a result of the Data Breach, Plaintiff Lee anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Lee is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

#### V. CLASS ALLEGATIONS

88. Plaintiff brings this action on behalf of himself and, pursuant to Haw. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

All persons in the United States whose PII was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives and officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

89. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that approximately 20,889 individuals comprise the Class and were affected by the Data Breach. The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.



90. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

- a. Whether Defendant's data security and retention policies were unreasonable;
- b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;
- c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;
- d. Whether Defendant breached any legal duties in connection with the Data Breach;
- e. Whether Defendant's conduct was intentional, reckless, willful or negligent;
- f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;
- g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;
- h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct; and
- i. Whether Plaintiff and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

91. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their PII compromised in the Data Breach. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

92. Adequacy: Plaintiff is an adequate representative because his interests do not materially or irreconcilably conflict with the interests of the Class he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and intends

to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

93. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff 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 the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, *inter alia*, Defendant's records and databases.

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

### **CAUSES OF ACTION**

#### **COUNT I — Negligence** **(By Plaintiff on behalf of the Class)**

95. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

96. This count is brought on behalf of all Class members.

97. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendant collected.

98. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its cyber networks and systems, and the personnel responsible for them, adequately protected the PII that Defendant collected.

99. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

100. Defendant owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

101. Defendant solicited, gathered, and stored the PII belonging to Plaintiff and the Class.

102. Defendant knew or should have known it inadequately safeguarded this information.

103. Defendant knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and Class members, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

104. Defendant had a special relationship with Plaintiff and Class members. Plaintiff's and Class members' highly sensitive PII and financial information was entrusted to Defendant on the understanding that adequate security precautions would be taken to protect the PII and financial information. Moreover, only Defendant had the ability to protect its systems and the PII stored on them from attack.

105. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff, Class members, and their PII. Defendant's misconduct included failing to: (1) secure its systems, servers and networks, despite knowing their vulnerabilities, (2) comply with industry standard security

practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

106. Defendant breached its duties to Plaintiff and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the PII belonging to Plaintiff and the Class.

107. Defendant breached its duties to Plaintiff and the Class by creating a foreseeable risk of harm through the misconduct previously described.

108. Defendant breached the duties it owed to Plaintiff and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

109. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII belonging to Plaintiff and the Class so that Plaintiff and the Class can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

110. Defendant breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and Class members that their PII had been improperly acquired or accessed.

111. Defendant breached its duty to timely notify Plaintiff and Class members of the Data Breach by failing to provide direct notice to Plaintiff and the Class concerning the Data Breach until on or about April 5, 2023.

112. As a direct and proximate result of Defendant's conduct, Plaintiff and the Class have suffered a drastically increased risk of identity theft, relative to both the time period before

the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

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

**COUNT II — Negligence *Per Se***  
**(By Plaintiff on behalf of the Class)**

114. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

115. This count is brought on behalf of all Class members.

116. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

117. Under Hawaii's Security Breach of Personal Information law (“HSB”), “any business that . . . maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license . . . shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach. . . .” Haw. Rev. Stat. § 487N-2(b).

118. In addition to the Hawai'i and federal rules and regulations, other states and jurisdictions where victims of the Data Breach are located require that Defendant protect PII from unauthorized access and disclosure, and timely notify the victim of a data breach.

119. Defendant violated HSB and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly

unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach, and the exposure of Plaintiff's and Class members' sensitive PII.

120. Defendant's violations of HSB, Section 5 of the FTC Act, and other applicable statutes, rules, and regulations constitutes negligence *per se*.

121. Plaintiff and the Class are within the category of persons HSB and the FTC Act were intended to protect.

122. The harm that occurred as a result of the Data Breach described herein is the type of harm HSB and the FTC Act were intended to guard against.

123. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT III — Breach of Implied Contract**  
**(By Plaintiff on behalf of the Class)**

124. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

125. This count is brought on behalf of all Class members.

126. Plaintiff and the Class provided Defendant with their PII and financial information.

127. As a regular part of its business operations, Defendant requires that employees and consumers provide to Defendant confidential and sensitive information, including their PII and financial information.

128. Plaintiff and Class members provided their PII, financial information, and other confidential and sensitive information in order to obtain services from Defendant, including employment and/or financial services.

129. By providing their PII and financial information, and upon Defendant's acceptance of such information, Plaintiff and the Class, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

130. The implied contracts between Defendant and Plaintiff and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII and financial information. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

131. The implied contracts for data security also obligated Defendant to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII and financial information.

132. Defendant breached the implied contracts by failing to take, develop, and implement adequate policies and procedures to safeguard, protect, and secure the PII and financial information belonging to Plaintiff and Class members; allowing unauthorized persons to access Plaintiff's and Class members' PII; and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

133. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to suffer injuries as detailed above due to the continued risk of exposure of their PII and financial information in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

**COUNT IV — Bailment**  
**(By Plaintiff on behalf of the Class)**

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

135. This count is brought on behalf of all Class members.

136. Plaintiff's and Class members' PII was provided to Defendant.

137. In delivering their PII, Plaintiff and Class members intended and understood that their PII would be adequately safeguarded and protected.

138. Defendant accepted Plaintiff's and Class members' PII.

139. By accepting possession of Plaintiff's and Class members' PII, Defendant understood that Plaintiff and the Class expected their PII to be adequately safeguarded and protected. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

140. During the bailment (or deposit), Defendant owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their PII.

141. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII.

142. Defendant further breached its duty to safeguard Plaintiff's and Class members' PII by failing to timely notify them that their PII had been compromised as a result of the Data Breach.

143. Defendant failed to return, purge, or delete the PII belonging to Plaintiff and Class members at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

144. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and the Class suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.



145. As a direct and proximate result of Defendant's breach of its duty, Plaintiff's and Class members PII that was entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

**COUNT V — Intrusion Upon Seclusion**  
**(By Plaintiff on behalf of the Class)**

146. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

147. This count is brought on behalf of all Class members.

148. Plaintiff and Class members had a reasonable expectation of privacy in the PII that Defendant possessed and/or continues to possess.

149. By failing to keep Plaintiff's and Class members' PII safe, and by misusing and/or disclosing their PII to unauthorized parties for unauthorized use, Defendant invaded Plaintiff's and Class members' privacy by:

- a. Intruding into their private affairs in a manner that would be highly offensive to a reasonable person; and
- b. Publicizing private facts about Plaintiff and Class members, which is highly offensive to a reasonable person.

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

151. Defendant invaded Plaintiff's and Class members' right to privacy and intruded into Plaintiff's and Class members' private affairs by misusing and/or disclosing their private information without their informed, voluntary, affirmative, and clear consent.

152. As a proximate result of such misuse and disclosures, Plaintiff's and Class members' reasonable expectation of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiff's and Class members' protected privacy interests.

153. In failing to protect Plaintiff's and Class members' PII, and in misusing and/or disclosing their PII, Defendant has acted with malice and oppression and in conscious disregard of Plaintiff's and the Class members rights to have such information kept confidential and private, in failing to provide adequate notice, and in placing its own economic, corporate, and legal interests above the privacy interests of its employees and consumers. Plaintiff, therefore, seeks an award of damages, including punitive damages, on behalf of Plaintiff and the Class.

**COUNT VI — Unjust Enrichment**  
**(By Plaintiff on behalf of the Class)**

154. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

155. This count is brought on behalf of all Class members.

156. Plaintiff and the Class have an interest, both equitable and legal, in their PII and financial information that was collected and maintained by Defendant.

157. Defendant was benefitted by the conferral upon it of Plaintiff's and Class members' PII and by its ability to retain and use that information. Defendant understood that it was in fact so benefitted.

158. Defendant also understood and appreciated that Plaintiff's and Class members' PII and financial information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

159. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiff and Class members would not have provided their PII to Defendant, and Defendant would have been deprived of the competitive and economic advantages it enjoyed by falsely claiming that its data-security safeguards met reasonable standards. These competitive and economic advantages include, without limitation, wrongfully gaining consumers, gaining the reputational advantages conferred upon it by Plaintiff and Class members, collecting excessive

advertising and sales revenues as described herein, monetary savings resulting from failure to reasonably upgrade and maintain data technology infrastructures, staffing, and expertise raising investment capital as described herein, and realizing excessive profits.

160. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiff, the Class, and the public relating to the nature and scope of the data breach; its failure to employ adequate data security measures; its continued maintenance and use of the PII belonging to Plaintiff and Class members without having adequate data security measures; and its other conduct facilitating the theft of that PII) Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and the Class.

161. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class members' sensitive PII, while at the same time failing to maintain that information secure from intrusion.

162. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiff and the Class in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

163. The benefit conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain the benefit.

164. Defendant is therefore liable to Plaintiff and the Class for restitution in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically

the value to Defendant of the PII and financial information that was accessed and exfiltrated in the Data Breach and the profits Defendant receives from the use and sale of that information.

**COUNT VII — Violation of Hawaii’s Unfair Deceptive Acts or Practices Statute**  
**Deceptive Practices**

**Haw. Rev. Stat. §§ 480-2(a), 480-13(b)**  
**(By Plaintiff on behalf of the Class)**

165. Plaintiff incorporates and reallages all allegations above as if fully set forth herein.

166. This count is brought on behalf of all Class members.

167. Haw. Rev. Stat. § 480-2(a) of Hawaii’s Unfair Deceptive Acts or Practices Statute (“UDAP”) provides that “[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful.”

168. Defendant’s deceptive acts or practices in the conduct of business include, but are not limited to:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff’s and Class members’ PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff’s and Class members’ PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff’s and Class members’ PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff’s and Class members’ PII;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff’s and Class members’ PII;

- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and
- h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

169. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout the United States.

170. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff's and Class members' PII. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiff's and Class members' PII and other Defendant data was vulnerable.

171. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

172. Defendant also had exclusive knowledge about the length of time that it maintained individuals' PII after they stopped using services that necessitated the transfer of that PII to Defendant.

173. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices, and regarding the security of the sensitive PII and financial information. For example, even though Defendant has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' PII was vulnerable as a result, Defendant failed

to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. Defendant also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former employees' and consumers' PII and other records. Likewise, during the days and weeks following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

174. Defendant had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiff's and Class members' PII and financial information.

175. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former employees' and consumers' PII.

176. Had Defendant disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' PII without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII.

177. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

178. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their PII;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;
- f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- g. damages to and diminution in value of their personal information entrusted to Defendant, and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and
- h. the continued risk to their PII, 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 data in its possession.

179. Defendant is engaged in "the conduct of any trade or commerce" because Defendant's acts and omissions were done in the course of Defendant's business of marketing, offering for sale, and selling goods that affect trade and commerce.

180. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages and treble damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

**COUNT VIII — Violation of Hawaii's Unfair Deceptive Acts or Practices Statute**  
**Unfair Practices**

**Haw. Rev. Stat. §§ 480-2(a), 480-13(b)**

**(By Plaintiff on behalf of the Class)**

181. Plaintiff incorporates and reallages all allegations above as if fully set forth herein.

182. This count is brought on behalf of all Class members.

183. Haw. Rev. Stat. § 480-2(a) of Hawaii's Unfair Deceptive Acts or Practices Statute ("UDAP") provides that "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."

184. Defendant engaged in "unfair or deceptive acts or practices" by failing to take sufficient and reasonable measures to safeguard their data security systems and protect Plaintiff's and Class members' highly sensitive personal information and financial data from unauthorized access despite representing to Plaintiff and the Class that Defendant would do so. Defendant's failure to maintain adequate data protections subjected Plaintiff's and the Class' nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

185. Defendant's unfair acts or practices in the conduct of business include, but are not limited to:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;



- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and
- h. Failing to promptly and adequately notify Plaintiff and the Class that their PII was accessed by unauthorized persons in the Data Breach.

186. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as the HSB and the FTC Act.

187. The injuries suffered by Plaintiff and the Class greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and the Class should have reasonably avoided.

188. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and the Class as a direct result of Defendant's unfair acts and practices as set forth herein include, without limitation:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their PII;
- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

- d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;
- e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;
- f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;
- g. damages to and diminution in value of their personal information entrusted to Defendant, and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and
- h. the continued risk to their PII, 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 data in its possession.

189. Defendant is engaged in “the conduct of any trade or commerce” because Defendant’s acts and omissions were done in the course of Defendant’s business of marketing, offering for sale, and selling goods that affect trade and commerce.

190. Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages and treble damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys’ fees and costs; and any other relief that is just and proper.

///

///

**COUNT IX — Violation of Hawaii’s Uniform Deceptive Trade Practices Act**  
**Haw. Rev. Stat. §§ 481A-2, 481A-3(a), 481A-3(a)(4), 481 A-3(a)(7), and 481A-3(a)(12)**  
**(By Plaintiff on behalf of the Class)**

191. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

192. This count is brought on behalf of all Class members.

193. Hawaii’s Uniform Deceptive Trade Practices Act (“UDTPA”) creates a cause of action against persons engaging in deceptive acts or practices “in the course of the person’s business . . . .” HRS § 481A-3(a).

194. Defendant is a “[p]erson” under the statute’s definition because Defendant is a “corporation.” HRS § 481A-2.

195. Deceptive practices include a business’s use of “deceptive representations . . . in connection with goods or services[,]” “represent[at]ions that goods or services are of a particular standard . . . if they are of another[,]” and “any other conduct which similarly creates a likelihood of confusion or of misunderstanding.” HRS §§ 481A-3(a)(4), 481A-3(a)(7), 481A-3(a)(12).

196. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant’s relevant acts, practices and omissions complained of in this action were done in the course of Defendant’s business of marketing, offering for sale, and selling goods and services throughout the United States.

197. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiff’s and Class members’ PII. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant’s security policies were substandard and deficient, and that Plaintiff’s and Class members’ PII and other Defendant data was vulnerable.

198. Defendant had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

199. Defendant also had exclusive knowledge about the length of time that it maintained individuals' PII after they stopped using services that necessitated the transfer of that PII to Defendant.

200. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices, and regarding the security of the sensitive PII and financial information. For example, even though Defendant has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiff's and Class members' PII was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from, Plaintiff, Class members and the public. Defendant also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former employees' and consumers' PII and other records. Likewise, during the days and weeks following the Data Breach, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

201. Defendant had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiff's and Class members' PII and financial information.

202. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former employees' and consumers' PII.

203. Had Defendant disclosed to Plaintiff and the Class that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' PII without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII.

204. Accordingly, Plaintiff and Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

205. Plaintiff and the Class members seek declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

**COUNT X — Violation of Hawaii's Security Breach of Personal Information**  
**Haw. Rev. Stat. § 487N-2(b)**  
**(By Plaintiff on behalf of the Class)**

206. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

207. This count is brought on behalf of all Class members.

208. Haw. Rev. Stat. § 487N-2(b) of Hawaii's Security Breach of Personal Information law ("HSB") provides that "[a]ny business located in Hawaii . . . that maintains or possesses records or data containing personal information of residents of Hawaii that the business does not own or license . . . shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach . . . ."

209. Defendant is a "business located in Hawaii" that "possesses records or data containing personal information of residents of Hawaii" for purposes of this statute because

Defendant is a financial entity that collected and stored Plaintiff's and other Hawai'i residents' PII as part of its business activities.

210. Defendant failed to comply with the requirements of Haw. Rev. Stat. § 487N-2(b) because Defendant did not immediately notify Plaintiff and the Class of the Data Breach. To the contrary, despite discovering the Data Breach on March 15, 2023, Defendant waited almost *one month* to notify Plaintiff and the Class, sending a notice on or around April 5, 2023.

211. As a result, Plaintiff and the Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendant, as follows:

- A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Hawaii Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;
- B. That Plaintiff be granted the declaratory relief sought herein;
- C. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;
- D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;
- E. That the Court award Plaintiff and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;
- F. That the Court award Plaintiff and the Class members damages three times the amount of actual damages, as permitted by Haw. Rev. Stat. § 480-13;
- G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

- H. That the Court award pre- and post-judgment interest at the maximum legal rate;
- I. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and
- J. That the Court grant all other relief as it deems just and proper.

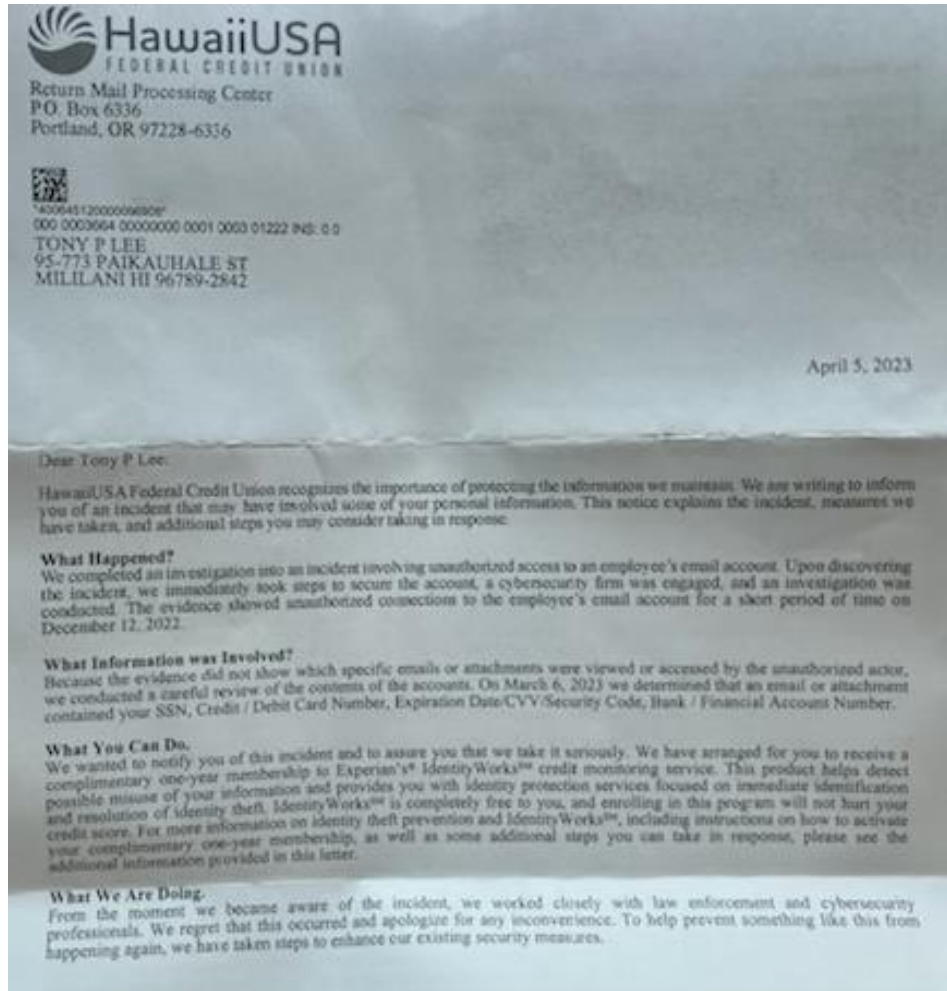
DATED: Honolulu, Hawai'i, April 28, 2023.

*/s/ Robert M. Hatch*

---

MARGERY S. BRONSTER  
ROBERT M. HATCH  
NOELLE E. CHAN  
DANIEL O. HERRERA  
NICKOLAS J. HAGMAN

Attorneys for Plaintiff TONY LEE  
and the Proposed Class





**IN THE CIRCUIT COURT OF THE FIRST CIRCUIT**

**STATE OF HAWAI‘I**

TONY LEE, individually, and on behalf of all  
others similarly situated,

Plaintiff,

v.

HAWAIIUSA FEDERAL CREDIT UNION,

Defendant.

Case No. \_\_\_\_\_

**DEMAND FOR JURY TRIAL**

**DEMAND FOR JURY TRIAL**

Plaintiff, on behalf of himself and the putative Class, demands a trial by jury on all issues so triable.

DATED: Honolulu, Hawai‘i, April 28, 2023.

*/s/ Robert M. Hatch*

\_\_\_\_\_  
MARGERY S. BRONSTER

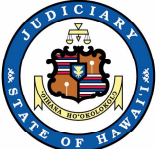

ROBERT M. HATCH

NOELLE E. CHAN

DANIEL O. HERRERA

NICKOLAS J. HAGMAN

Attorneys for Plaintiff TONY LEE  
and the Proposed Class

|  |  |   |
|--|--|---|
| <b>STATE OF HAWAI'I<br/>CIRCUIT COURT OF THE<br/>FIRST CIRCUIT</b>   | <b>SUMMONS<br/>TO ANSWER CIVIL COMPLAINT</b>   | CASE NUMBER                                     |
| PLAINTIFF<br>TONY LEE, individually, and on behalf<br>of all others similarly situated,  | VS.  | DEFENDANT(S)<br>HAWAIIUSA FEDERAL CREDIT UNION, |
| PLAINTIFF'S NAME & ADDRESS, TEL. NO.<br><br>Margery S. Bronster #4750/Robert M. Hatch #7724<br>Noelle E. Chan #11280<br>1003 Bishop Street, Suite 2300<br>Honolulu, Hawai'i 96813<br>Telephone: (808) 524-5644   |  |   |
| <p><b>TO THE ABOVE-NAMED DEFENDANT(S)</b></p> <p>You are hereby summoned and required to file with the court and serve upon</p> <p>Margery S. Bronster/Robert M. Hatch/Noelle E. Chan<br/>                 1003 Bishop Street, Suite 2300<br/>                 Honolulu, Hawaii 96813</p> <hr/> <p>plaintiff's attorney, whose address is stated above, an answer to the complaint which is herewith served upon you, within 20 days after service of this summons upon you, exclusive of the date of service. If you fail to do so, judgment by default will be taken against you for the relief demanded in the complaint.</p> <p><b>THIS SUMMONS SHALL NOT BE PERSONALLY DELIVERED BETWEEN 10:00 P.M. AND 6:00 A.M. ON PREMISES NOT OPEN TO THE GENERAL PUBLIC, UNLESS A JUDGE OF THE ABOVE-ENTITLED COURT PERMITS, IN WRITING ON THIS SUMMONS, PERSONAL DELIVERY DURING THOSE HOURS.</b></p> <p><b>A FAILURE TO OBEY THIS SUMMONS MAY RESULT IN AN ENTRY OF DEFAULT AND DEFAULT JUDGMENT AGAINST THE DISOBEYING PERSON OR PARTY.</b></p> |  |   |
| The original document is filed in the Judiciary's electronic case management system which is accessible via eCourt Kokua at: <a href="http://www.courts.state.hi.us">http://www.courts.state.hi.us</a>   | <p><b>Effective Date of 28-Oct-2019</b><br/> <b>Signed by: /s/ Patsy Nakamoto</b><br/> <b>Clerk, 1st Circuit, State of Hawai'i</b></p>  |   |
| <div style="display: flex; align-items: center;">  <p>In accordance with the Americans with Disabilities Act, and other applicable state and federal laws, if you require a reasonable accommodation for a disability, please contact the ADA Coordinator at the Circuit Court Administration Office on OAHU- Phone No. 808-539-4400, TTY 808-539-4853, FAX 539-4402, at least ten (10) working days prior to your hearing or appointment date.</p> </div>  |  |   |