

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
E-mail: mbronster@bfrhawaii.com
rhatch@bfrhawaii.com
nchan@bfrhawaii.com

**MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC**

GARY M. KLINGER (*pro hac vice* to be
submitted)
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
E-mail: gklinger@milberg.com

Attorneys for Plaintiffs

IN THE CIRCUIT COURT OF THE FIRST CIRCUIT

STATE OF HAWAI'I

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

Plaintiffs,

v.

HAWAIIUSA FEDERAL CREDIT UNION,

Defendant.

**CAFFERTY CLOBES MERIWETHER &
SPRENGEL LLP**

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
nhagman@caffertyclobes.com

Electronically Filed
FIRST CIRCUIT
1CCV-24-0000154
30-JAN-2024
03:30 PM
Dkt. 1 CMPS

Case No.

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

Plaintiffs Joseph Smith and Tony Lee (collectively, “Plaintiffs”), individually, and on behalf of all others similarly situated, bring this action against HawaiiUSA Federal Credit Union (“HawaiiUSA” or “Defendant”), by and through their attorneys, and allege, based upon personal knowledge as to their own actions and their counsels’ investigation, and based upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. HawaiiUSA 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.¹

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 financial account information including security codes, access codes, passwords, or PINs (“Private Information”).²

3. Upon information and belief, former and current customers of Defendant’s are required to entrust Defendant with this sensitive, non-public Private Information, without which Defendant could not perform its regular business activities, in order to apply for financial services from Defendant. Defendant retains this information for many years, even after the consumer

¹ *Services*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/Banking/Personal/Services>.

² *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 July 28, 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 July 28, 2023).

relationship has ended. Defendant's employees and customers provide this information under the expectation that Defendant, a sophisticated financial services provider, will safeguard their highly valuable Private Information.

4. By obtaining, collecting, using and deriving a benefit from the Private Information of Plaintiffs and Class members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Defendant, however, failed to invest in adequate data security, thereby allowing hackers to exfiltrate the highly-sensitive Private Information of approximately 21,441 individuals, including Plaintiffs' and Class members' Private Information.³ 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 Private Information.⁴

6. 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 Private Information for approximately 21,441 individuals (the "Data Breach").⁵

7. Defendant failed to detect the breach until much later, admitting that it did not discover the full extent of the Data Breach until on or around March 6, 2023, more than *three*

³ *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aevier/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed July 28, 2023).

⁴ *Id.*

⁵ *Id.*

months after the breach occurred.⁶ Defendant notified affected individuals, including Plaintiffs, on or around April 7, 2023, almost *four* months after unauthorized individuals accessed Plaintiffs' and current and former employees' and consumers' highly sensitive Private Information that is stored on Defendant's systems.⁷

8. Defendant's failure to promptly notify Plaintiffs and Class members that their Private Information 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 Private Information before Plaintiffs and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiffs and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

9. 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 Private Information and financial information; and to timely detect and provide adequate notice of the Data Breach to affected individuals. Due to Defendant's failures, Plaintiffs and approximately 21,441 individuals suffered substantial harm and injury.

10. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiffs' and

⁶ *Id.*

⁷ 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 July 28, 2023).

Class members' Private Information was targeted, 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. Plaintiffs and Class members face the real, present, and continuing danger of identity theft and misuse of their Private Information, especially because their Private Information was specifically targeted by the malevolent actors that carried out this Data Breach.

11. Plaintiffs and Class members suffered injuries as a result of Defendant's conduct including, but not limited to: fraudulent tax returns being filed under victims' name; lost or diminished value of Plaintiffs' and Class members' Private Information; out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; 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 Private Information, 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 Private Information. These risks will remain for the lifetimes of Plaintiffs and the Class.

12. Accordingly, Plaintiffs bring this action on behalf of all those similarly situated to seek relief from Defendant's failure to reasonably safeguard Plaintiffs' and Class members' Private Information; its failure to reasonably provide timely notification that Plaintiffs' and Class

members' Private Information had been compromised by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiffs and Class members concerning the status, safety, location, access, and protection of their Private Information.

II. PARTIES

Plaintiff Joseph Smith

13. Plaintiff Joseph Smith is a resident and citizen of Missouri, residing in St. Louis, Missouri.

14. Plaintiff Smith received Defendant's Notice of Data Breach (the "Notice"), dated April 5, 2023, via U.S. Mail.

Plaintiff Tony Lee

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

16. Plaintiff Lee received Defendant's Notice, dated April 5, 2023, via U.S. Mail.

Defendant HawaiiUSA Federal Credit Union

17. Defendant HawaiiUSA Federal Credit Union is a financial and banking services cooperative organized under the laws of Hawai'i with its principal place of business at 1226 College Walk, Honolulu, Hawai'i 96817.⁸ Defendant operates more than a dozen branches, all of which are located in the Hawaiian Islands.

III. JURISDICTION AND VENUE

18. This Court has jurisdiction over this action pursuant to Hawaii Revised Statutes § 603-21.5. HawaiiUSA Federal Credit Union purposefully availed itself of the laws, protections,

⁸ *HawaiiUSA Federal Credit Union*, Hawaii.gov, <https://hbe.ehawaii.gov/documents/trade.html?fileNumber=485760ZZ&certificate=4263242>.

and advantages of doing business in the City and County of Honolulu, and the events and transactions giving rise to the cause of action alleged herein occurred in Hawai‘i.

19. 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 Hawaii.

IV. FACTUAL ALLEGATIONS

A. **Defendant – Background**

20. 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 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.⁹ 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.”¹⁰

21. As part of its financial and business operations, Defendant requires that employees and consumers provide their Private Information and financial information. Defendant collects, maintains, and stores highly sensitive Private Information, 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.

22. On information and belief, Defendant made promises and representations to its customers and employees, including Plaintiffs and Class members, that the Private Information

⁹ *Bank*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/Banking>; *Borrow*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com/Loans>.

¹⁰ *HawaiiUSA Federal Credit Union*, HawaiiUSA Federal Credit Union, <https://www.hawaiiusafcu.com>.

collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

23. Defendant derived a substantial economic benefit from collection Plaintiffs' and Class members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

24. 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 Private Information of approximately 21,441 current and former employees and consumers.¹¹

25. Current and former employees and customers of Defendant, such as Plaintiffs and the Class, made their Private Information 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 Private Information.

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

¹¹ *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aevier/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml>.

B. The Data Breach

27. Defendant disclosed in a Notice sent on or about April 5, 2023, to Plaintiffs 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**. Defendant further acknowledged that the unauthorized party was able to exfiltrate Plaintiffs’ and Class members’ Private Information. *See* Exhibit A.

28. Omitted from the Notice is the date that Defendant discovered the Data Breach, the date that Defendant began its investigation, the date that Defendant concluded its investigation, any clarifying details on the sensitive Private Information that the perpetrator(s) obtained, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. Instead, Defendant simply stated that it performed a “careful review of the contents of the accounts,” and on March 6, 2023, determined that Private Information was accessed during the Data Breach. *See* Exhibit A.

29. Despite discovering the Data Breach prior to March 6, 2023, and only determining the extent of the Data Breach on March 6, 2023, and confirming that the unauthorized actor may have accessed and exfiltrated employees’ and consumers’ Private Information, 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.

30. 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 Private Information belonging to over 21,441 current and former employees and customers of Defendant.

31. Defendant failed to disclose to Plaintiffs and other victims of the Data Breach when the unauthorized third party first gained access to Defendant's systems, how long the unauthorized actor had access to Plaintiffs' and Class members' information, the date that Defendant concluded its investigation, any clarifying details on the sensitive Private Information the perpetrator obtained, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class members, who retain a vested interest in ensuring that their Private Information remains protected.

32. Defendant's April 5, 2023 "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

33. On information and belief, Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining concerning Plaintiffs and Class members, such as encrypting the information or deleting it when it is no longer necessary, causing the exposure of their Private Information.

34. Plaintiffs further believe that their Private Information, as well as that of Class members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

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

35. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”¹²

36. 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 Private Information, and permanently deleting sensitive data and Private Information when it is no longer necessary to store such data.

37. To be sure, collecting, maintaining, and protecting Private Information 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 before March 6, 2023.¹³

38. 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 Plaintiffs' and Class members' Private Information, or even the full extent of the Private Information that was accessed during the Data Breach.

39. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information.

40. Defendant's failure to properly safeguard Plaintiffs' and Class members' Private Information allowed the unauthorized actors to access this highly valuable information, and Defendant's failure to timely notify Plaintiffs and other victims of the Data Breach that their P

¹² See How to Protect Your Networks from RANSOMWARE, Federal Bureau of Investigation, at p. 3, <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-forcisos.pdf/view> (last accessed July 28, 2023).

¹³ *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aevviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml> (last accessed July 28, 2023).

Private Information was accessed served only to exacerbate the harms they suffered as a direct and proximate result thereof because it precluded them from taking meaningful steps to safeguard their identities prior to the further dissemination and misuse of their Private Information.

41. 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 Private Information and financial information.

42. First, Defendant failed to timely discover the Data Breach and immediately secure its computer systems to protect its current and former employees' and consumers' Private Information and financial information. It instead allowed unauthorized actors to continue to have access to its computer systems for an unknown period of time, and did not determine the full extent of the Data Breach until March 6, 2023.¹⁴

43. Second, Defendant failed to timely notify affected individuals, including Plaintiffs and Class members, that their highly sensitive Private Information 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 Private Information had been compromised.

44. Third, Defendant made no effort to protect Plaintiffs 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, Plaintiffs' and Class members' Private Information, including their Social Security numbers, cannot be changed and will remain at risk long beyond one year. As a result, Plaintiffs and the

¹⁴ *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/dcd41e8a-42b1-4ce0-834d-98e626d04333.shtml>.

Class will remain at a heightened and unreasonable risk of identity theft for the remainder of their lives.

45. Further, Defendant likely failed to adequately protect current and former employees' and consumers' Private Information 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.

46. In short, Defendant's myriad failures, including the failure to timely detect the Data Breach and notify Plaintiffs 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 Plaintiffs' and Class members' Private Information 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 to Victims

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

48. 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 2021.¹⁵

49. 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 1,802.¹⁶ 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.¹⁷

50. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

¹⁵ *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.

¹⁶ *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>.

¹⁷ *Id.*

51. Data breaches are a constant threat because Private Information 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.¹⁸

52. 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.”¹⁹

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.”²⁰

¹⁸ *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>.

¹⁹ 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>.

²⁰ *Id.*

53. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

54. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

55. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

56. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.²¹

²¹ "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground*

57. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

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

59. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like driver’s license numbers) of Plaintiffs and the other Class Members.

60. Thus, even if certain information (such as driver’s license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

61. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

62. 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 Private Information know the importance of protecting that information from

Stolen From Texas Life Insurance Firm, Krebs on Security (Sep. 18, 2014), [https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\].](https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-/)

unauthorized disclosure. Indeed, on information and belief, Defendant was aware of highly publicized security breaches where Private Information and protected financial information was accessed by unauthorized cybercriminals.

63. Additionally, as companies became more dependent on computer systems to run their business,²² *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.²³

64. 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.

65. 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.

66. 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 Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs’ and Class members’ Private Information can easily obtain Plaintiffs’ and Class members’ tax returns or open fraudulent credit card accounts in their names.

²²<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>

²³ <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>

67. Based on the foregoing, the Social Security numbers compromised in the Data Breach hold significant value on the dark web.²⁴ The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

68. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class members as a result of a breach.

69. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class members from being compromised.

70. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class members and of the foreseeable consequences that would occur if Defendant’s data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class members as a result of a breach.

71. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant’s server(s), amounting to potentially thousands of individuals’ detailed Private Information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

72. To date, Defendant has offered its consumers *only one year* of identity theft monitoring services. The offered services are inadequate to protect Plaintiffs and the Class from

²⁴ 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>.

the threats they will face for years to come, particularly in light of the Private Information at issue here.

73. Defendant's offer of credit and identity monitoring establishes that Plaintiffs' and Class members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

74. 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 Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the Class from misappropriation. As a result, the injuries to Plaintiffs 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 Private Information

75. Defendant has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiffs' and Class members' Private Information. 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 Private Information and financial records. Plaintiffs and Class members provided, and Defendant obtained, their Private Information on the understanding that their Private Information would be protected and safeguarded from unauthorized access or disclosure.

76. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²⁵ 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.”²⁶

77. 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.²⁷

78. 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.²⁸ The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct security problems.²⁹ 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

²⁵ 17 C.F.R. § 248.201 (2013).

²⁶ *Id.*

²⁷ *Start With Security*, Federal Trade Commission (June 2015), available at <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

²⁸ *Protecting Personal Information: A Guide for Business*, Federal Trade Comm’n (October 2016), available at <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business>.

²⁹ *Id.*

of data being transmitted from the system; and have a response plan ready in the event of a breach.³⁰ 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.

79. Here, at all relevant times, Defendant was fully aware of its obligation to protect the Private Information and protected financial information of its current and former employees and consumers, including Plaintiffs 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' Private Information in order to operate its business.

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

81. 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.

82. Further, Defendant had a duty to promptly notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons.

³⁰ *Id.*

F. Defendant Violated FTC and Industry Standard Data Protection Protocols

83. The FTC rules, regulations, and guidelines obligate businesses to protect Private Information from unauthorized access or disclosure by unauthorized persons.

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

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

86. Unfortunately, Defendant failed to comply with FTC rules, regulations and guidelines, and industry standards concerning the protection and security of Private Information. 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' Private Information, 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' Private Information;
- 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 Private Information 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 Private Information 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' Private Information.

87. 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 Private Information 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 Failed to Comply with Industry Standards

88. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

89. Several best practices have been identified that, at a minimum, should be implemented by financing companies in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multilayer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access

sensitive data. HawaiiUSA failed to follow these industry best practices, including a failure to implement multi-factor authentication.

90. Other best cybersecurity practices that are standard in the financing industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. HawaiiUSA failed to follow these cybersecurity best practices, including failure to train staff.

91. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

92. These foregoing frameworks are existing and applicable industry standards in the financing industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

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

93. Defendant purports to care about data security and safeguarding Private Information and represents that it will keep secure and confidential the Private Information belonging to its current and former employees and consumers.

94. Plaintiffs' and Class members' Private Information and financial information was provided to Defendant in reliance on its promises and self-imposed obligations to keep Private Information and financial information confidential, and to secure the Private Information and financial information from unauthorized access by malevolent actors. Defendant failed to do so.

95. The length of the Data Breach also demonstrates that Defendant failed to safeguard Private Information 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.

96. 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.

97. 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.

I. Plaintiffs and the Class Suffered Harm Resulting from the Data Breach

98. Like any data hack, the Data Breach presents major problems for all affected.³¹

³¹ Paige Schaffer, *Data Breaches' Impact on Consumers*, Insurance Thought Leadership (July 29, 2021), available at <https://www.insurancethoughtleadership.com/cyber/data-breaches-impact-consumers>.

99. 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 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.”³²

100. The ramifications of Defendant’s failure to properly secure the Private Information of Plaintiffs and Class members, are severe.³³ 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.

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

102. Furthermore, Private Information 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.

103. Accordingly, Defendant’s wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the Class at an imminent, immediate, and continuing increased risk of identity theft and identity fraud.³⁴ 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’ Private Information will do so at a later date or re-sell it.

³²*Warning Signs of Identity Theft*, Federal Trade Comm’n, available at <https://www.identitytheft.gov/#/Warning-Signs-of-Identity-Theft>.

³³ *Cost of a Data Breach Report 2023*, IBM, available at <https://www.ibm.com/reports/data-breach>.

³⁴ *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>.

104. In response to the Data Breach, Defendant offered to provide certain individuals whose Private Information 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 Plaintiffs and Class members by Defendant's failures.

105. 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 Private Information.

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

- a. Theft of Private Information, 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 Private Information 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 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 Private Information is exposed for theft and sale on the dark web; and
- f. The loss of Plaintiffs' and Class members' privacy.

107. Furthermore, Defendant's poor data security deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendant for financial services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class members received financial services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

108. Plaintiffs and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their Private Information and protected financial information being accessed by cybercriminals, risks that will not abate within a mere one year: the unauthorized access of Plaintiffs' and Class members' Private Information, especially their Social Security numbers, puts Plaintiffs 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 Plaintiffs and Class members have suffered and will continue to suffer as a result of the Data Breach.

109. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure Private Information and financial information, Plaintiffs 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.

110. Private Information is also a valuable property right.³⁵ Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts

³⁵ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009)

include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

111. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly \$200 billion.³⁶

112. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.³⁷

113. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.³⁸

114. Conversely sensitive Private Information can sell for as much as \$363 per record on the dark web according to the Infosec Institute.³⁹

115. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

³⁶ David Lazerus, *Shadowy Data Brokers Make the Most of their Invisibility Cloak*, LA Times (Nov. 5, 2019), <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

³⁷ *World Data Exchange*, World Data Exchange, available at: <https://worlddataexchange.com>.

³⁸ Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, available at <https://computermobilepanel.nielsen.com/ui/US/en/faqen.html>.

³⁹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>.

116. Plaintiffs retain 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 themselves and similarly situated individuals whose Private Information and financial information was accessed in the Data Breach.

117. 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 Plaintiffs 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." Exhibit A.

J. Plaintiff Smith's Experience

118. Plaintiff Smith was a customer of Defendant's from approximately 2014 through 2016.

119. In order to open a financial account or otherwise use Defendant's financial services, Plaintiff Smith was required to provide his Private Information to Defendant, including his name, Social Security number, and financial information.

120. Plaintiff Smith provided his Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Smith had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain his sensitive Private Information.

121. At the time of the Data Breach—on or about December 12, 2022—Defendant retained Plaintiff Smith's Private Information in its system.

122. Plaintiff Smith is very careful about sharing his sensitive Private Information and stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

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

124. In the Notice that Plaintiff Smith received sometime after April 5, 2023, Defendant informed Plaintiff Smith that an authorized 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 Plaintiff Smith's Private Information, including his Social Security number and other financial information. Defendant advised Plaintiff Smith to, among other things, access and review his credit reports and consider placing a freeze on his credit account.

125. As a result of the Data Breach, Plaintiff Smith 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 Smith has spent several hours dealing with the Data Breach, valuable time Plaintiff Smith otherwise would have spent on other activities, including, but not limited to, work and/or recreation.

126. Following the Data Breach, Plaintiff Smith suffered from identity theft when fraudulent tax returns were filed under his name.

127. Upon information and believe, Plaintiff Smith has further experienced an increase in spam calls, texts, and emails, which he believes is related to the Data Breach.

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

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

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

131. Upon information and belief, Plaintiff Smith continues to suffer actual injuries and a continued and increased risk to his Private Information, which (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

132. As a result of the Data Breach, Plaintiff Smith 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 Smith is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

K. Plaintiff Lee's Experience

133. Plaintiff Lee is currently, and has been for over ten years, a customer of Defendant. Specifically, Plaintiff Lee 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.

134. In order to open a financial account or otherwise use Defendant's financial services, Plaintiff Lee was required to provide his Private Information to Defendant, including his name, Social Security number, and financial information.

135. Plaintiff Lee provided his Private Information to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Lee had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain his sensitive Private Information.

136. Plaintiff Lee is very careful about sharing his sensitive Private Information and stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

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

138. In the Notice that Plaintiff Lee received sometime after April 5, 2023, Defendant informed Plaintiff Lee that an authorized 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 Plaintiff Lee's Private Information, including his Social Security number, credit and debit card number, bank and financial account number and other financial information. Defendant advised Plaintiff Lee to, among other things, access and review his credit reports and consider placing a freeze on his credit account.

139. 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.

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

141. As a result of the Data Breach, Plaintiff Lee has suffered anxiety due to the public dissemination of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information 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.

142. Plaintiff Lee suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, 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.

143. 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

144. Plaintiffs bring this action on behalf of themselves and, pursuant to Haw. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the Data Breach (the “Class”).

Excluded from the Class are Defendant, Defendant’s parents, subsidiaries, affiliates, executives, officers, and directors; and any judge assigned to this case as well as their immediate family members.

145. Plaintiffs reserve the right to modify, change or expand the Class definition after conducting discovery.

146. 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 Plaintiffs only through the discovery process, Plaintiffs believe, and on that basis allege, that approximately 21,441 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.

147. 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 Plaintiffs and Class members to safeguard their Private Information;
- 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 Plaintiffs' and Class members' Private Information;
- g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiffs' and Class members' Private Information and/or failing to timely and adequately notify Plaintiffs and Class members of the Data Breach;
- h. Whether Plaintiffs and Class members suffered damages as a result of Defendant's conduct; and
- i. Whether Plaintiffs and the Class are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

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

149. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class a whole, not on facts or law applicable only to Plaintiffs.

150. Adequacy: Plaintiffs are adequate representatives because their interests do not materially or irreconcilably conflict with the interests of the Class they seek to represent, they have retained counsel competent and highly experienced in complex class action litigation, and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the Class. Neither Plaintiffs nor their counsel have any interests that are antagonistic to the interests of other members of the Class.

151. Superiority and Manageability: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of 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.

152. The nature of this action and the nature of laws available to Plaintiffs and Class members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation. 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.

153. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

154. Adequate notice can be given to Class members directly using information maintained in Defendant's records.

155. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class members, Defendant may continue to refuse to

provide proper notification to Class members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

156. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

CAUSES OF ACTION

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

157. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

159. Defendant requires its customers, including Plaintiffs and Class members, to submit non-public Private Information in the ordinary course of providing financing services.

160. Plaintiffs and Class members entrusted Defendant with their Private Information for the purpose of securing financial or other services from Defendant.

161. Defendant owed a duty to Plaintiffs and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the Private Information that Defendant collected.

162. Defendant owed a duty to Plaintiffs 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 Private Information that Defendant collected.

163. Defendant owed a duty to Plaintiffs 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.

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

165. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of being employees and customers of Defendant.

166. Defendant solicited, gathered, and stored the Private Information belonging to Plaintiffs and the Class.

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

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

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

170. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs, Class members, and their Private Information. 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.

171. Defendant breached its duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate cyber networks and data security practices to safeguard the Private Information belonging to Plaintiffs and the Class.

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

173. Defendant breached the duties it owed to Plaintiffs and Class members by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of Private Information.

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

175. Defendant breached the duties it owed to Plaintiffs and the Class by failing to timely and accurately disclose to Plaintiffs and Class members that their Private Information had been improperly acquired or accessed.

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

177. As a direct and proximate result of Defendant's conduct, Plaintiffs 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.

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

179. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class members.

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

180. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

182. 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 Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

183. The GLBA required Defendant to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

184. Under Hawai'i's Security Breach of Personal Information law (“HSB”), “any business that . . . maintains or possesses records or data containing personal information of residents of Hawai'i 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).

185. 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 Private Information from unauthorized access and disclosure, and timely notify the victim of a data breach.

186. Defendant violated HSB, FTC, and GLBA rules and regulations obligating companies to use reasonable measures to protect Private Information 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 Private Information it obtained and stored, the foreseeable consequences of a Data Breach, and the exposure of Plaintiffs’ and Class members’ sensitive Private Information.

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

188. Plaintiffs and the Class are within the category of persons HSB, the FTC Act, and the GLBA were intended to protect.

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

190. As a direct and proximate result of Defendant’s negligence *per se*, Plaintiffs 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 Private Information in Defendant’s possession, and are entitled to compensatory and consequential damages in an amount to be proven at trial.

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

191. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

193. Plaintiffs and the Class provided Defendant with their Private Information and financial information in exchange for (among other things) Defendant's promise to protect their Private Information from unauthorized disclosure and to delete it once it was no longer required to maintain it.

194. As a regular part of its business operations, Defendant requires that employees and consumers provide Defendant with confidential and sensitive information, including their Private Information and financial information.

195. Plaintiffs and Class members provided their Private Information, financial information, and other confidential and sensitive information in order to obtain services from Defendant, including employment and/or financial services.

196. By providing their Private Information and financial information, and upon Defendant's acceptance of such information, Plaintiffs 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.

197. The implied contracts between Defendant and Plaintiffs and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiffs' and Class members' Private Information 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.

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

199. Plaintiffs and Class members fully and adequately performed their obligations under the implied contracts with Defendant.

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

201. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiffs 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 Private Information and financial information in Defendant's possession, and are entitled to compensatory and consequential damages in an amount to be proven at trial.

202. Plaintiffs and Class members are also entitled to nominal damages for the breach of implied contract.

203. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class members.

COUNT IV — Unjust Enrichment
(By Plaintiffs on behalf of the Class)

204. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

206. This count is pleaded in the alternative to the breach of contract claim above.

207. Plaintiffs and the Class have an interest, both equitable and legal, in their Private Information and financial information that was collected and maintained by Defendant.

208. Defendant was benefitted by the conferral upon it of Plaintiffs' and Class members' Private Information and by its ability to retain and use that information. Defendant profited from this benefit, as the transmission of Private Information to Defendant from Plaintiffs and Class member is an integral part of Defendant's business, without which it would be unable to offer financial services. Defendant understood that it was in fact so benefitted.

209. Defendant also understood and appreciated that Plaintiffs' and Class members' Private Information and financial information was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

210. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, Plaintiffs and Class members would not have provided their Private Information 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 Plaintiffs 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.

211. As a result of Defendant's wrongful conduct as alleged herein (including, among other things, its deception of Plaintiffs, 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 Private Information belonging to Plaintiffs and Class members without having adequate data security measures; and its other conduct facilitating the theft of that Private Information) Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class.

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

213. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiffs and Class members have no adequate remedy at law.

214. 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 Plaintiffs 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.

215. 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.

216. Defendant is therefore liable to Plaintiffs 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 Private Information 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 V — Violation of Hawaii’s Unfair Deceptive Acts or Practices Statute
Deceptive Practices
Haw. Rev. Stat. §§ 480-2(a), 480-13(b)
(By Plaintiffs on behalf of the Class)

217. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

219. Haw. Rev. Stat. § 480-2(a) of Hawai‘i’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.”

220. H.R.S. § 481A-3(a)(2) states that “[i]n construing this section, the courts and the office of consumer protection shall give due consideration to the rules, regulations, and decisions of the Federal Trade Commission and the federal courts interpreting section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)). H.R.S. § 480-2.

221. 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 Plaintiffs’ and Class members’ Private Information, 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 Plaintiffs' and Class members' Private Information, 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 Plaintiffs' and Class members' Private Information, 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 Plaintiffs' and Class members' Private Information;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;
- 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 Plaintiffs' and Class members' Private Information; and
- h. Failing to promptly and adequately notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

222. 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.

223. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs' and Class members' Private Information. 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 Plaintiffs' and Class members' Private Information and other Defendant data was vulnerable.

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

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

226. 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 Private Information 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 Plaintiffs' and Class members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from, Plaintiffs, 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' Private Information 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.

227. 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 Plaintiffs' and Class members' Private Information and financial information.

228. 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' Private Information.

229. Had Defendant disclosed to Plaintiffs 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 Plaintiffs' and Class members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

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

231. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs 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 Private Information;
- 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 Private Information 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 Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

232. 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.

233. Plaintiffs 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 Private Information without their consent; reasonable attorneys’ fees and costs; and any other relief that is just and proper.

COUNT VI — Violation of Hawaii’s Uniform Deceptive Trade Practices Act
Deceptive Practices

Haw. Rev. Stat. §§ 481A-2, 481A-3(a), 481A-3(a)(4), 481 A-3(a)(7), and 481A-3(a)(12)
(By Plaintiffs on behalf of the Class)

234. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

236. Hawai‘i’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).

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

238. 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).

239. 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.

240. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs’ and Class members’ Private Information. 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 Plaintiffs’ and Class members’ Private Information and other Defendant data was vulnerable.

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

242. Defendant also had exclusive knowledge about the length of time that it maintained individuals’ Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

243. 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 Private Information 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 Plaintiffs' and Class members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from Plaintiffs, 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' Private Information 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.

244. 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 Plaintiffs' and Class members' Private Information and financial information.

245. 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' Private Information.

246. Had Defendant disclosed to Plaintiffs 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 Plaintiffs' and Class members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

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

248. Plaintiffs and the Class seek declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys’ fees and costs; and any other relief that is just and proper.

COUNT VII — Violation of Hawai‘i’s Unfair Deceptive Acts or Practices Statute
Unfair Practices
Haw. Rev. Stat. §§ 480-2(a), 480-13(b)
(By Plaintiffs on behalf of the Class)

249. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

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

251. Haw. Rev. Stat. § 480-2(a) of Hawai‘i’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.”

252. 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 Plaintiffs’ and Class members’ highly sensitive personal information and medical data from unauthorized access despite representing to Plaintiffs and the Class that Defendant would do so. Defendant’s failure to maintain adequate data protections subjected Plaintiffs’ and the Class’s nonencrypted and nonredacted sensitive personal information to exfiltration and disclosure by malevolent actors.

253. 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 Plaintiffs’ and Class members’ Private Information, 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 Plaintiffs' and Class members' Private Information, 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 Plaintiffs' and Class members' Private Information, 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 Plaintiffs' and Class members' Private Information;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Private Information;
- 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 Plaintiffs' and Class members' Private Information; and
- h. Failing to promptly and adequately notify Plaintiffs and the Class that their Private Information was accessed by unauthorized persons in the Data Breach.

254. 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, HIPAA and the FTC Act.

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

256. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs 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 Private Information;
- 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 Private Information 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 Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

257. 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.

258. Plaintiffs 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 Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VIII — Violation of Hawaii's Security Breach of Personal Information
Haw. Rev. Stat. § 487N-2(b)
(By Plaintiff Lee on behalf of the Hawai'i Subclass)

259. Plaintiffs incorporate and reallege all allegations above as if fully set forth herein.

260. This count is brought on behalf of all Hawai'i Subclass members.

261. Haw. Rev. Stat. § 487N-2(b) of Hawai'i'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"

262. 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 Plaintiffs' and other Hawai'i residents' Private Information as part of its business activities.

263. Defendant failed to comply with the requirements of Haw. Rev. Stat. § 487N-2(b) because Defendant did not immediately notify Plaintiffs and the Subclass of the Data Breach. To the contrary, despite determining the extent of the Data Breach on March 6, 2023, Defendant waited almost *one month* to notify Plaintiffs and the Subclass, sending a notice on or around April 5, 2023.

264. As a result, Plaintiffs and Subclass 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 Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their 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 Hawai'i Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Counsel as Class Counsel;
- B. That Plaintiffs 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 Plaintiffs and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;
- E. That the Court award Plaintiffs and the Class members statutory damages, and punitive or exemplary damages, to the extent permitted by law;
- F. That the Court award Plaintiffs 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 Plaintiffs 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 January 30, 2024.

Respectfully Submitted,

/s/ Robert M. Hatch

Margery S. Bronster

Robert M. Hatch

Noelle E. Chan

BRONSTER FUJICHAKU ROBBINS

Gary M. Klinger (*pro hac vice to be submitted*)

MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN PLLC

Nickolas J. Hagman (*pro hac vice to be submitted*)

CAFFERTY CLOBES MERIWETHER &

SPRENGEL LLP

Attorneys for Plaintiffs and the Proposed Class



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336



4006412000009800
000 0003664 00000000 0001 0003 01222 940: 0 0

TONY P LEE
95-773 PAIKAUHALE ST
MILILANI HI 96789-2842

April 5, 2023

Dear Tony P Lee,

HawaiiUSA Federal Credit Union recognizes the importance of protecting the information we maintain. We are writing to inform you of an incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and additional steps you may consider taking in response.

What Happened?

We completed an investigation into an incident involving unauthorized access to an employee's email account. Upon discovering the incident, we immediately took steps to secure the account, a cybersecurity firm was engaged, and an investigation was conducted. The evidence showed unauthorized connections to the employee's email account for a short period of time on December 12, 2022.

What Information was Involved?

Because the evidence did not show which specific emails or attachments were viewed or accessed by the unauthorized actor, we conducted a careful review of the contents of the accounts. On March 6, 2023 we determined that an email or attachment contained your SSN, Credit / Debit Card Number, Expiration Date/CVV/Security Code, Bank / Financial Account Number.

What You Can Do.

We wanted to notify you of this incident and to assure you that we take it seriously. We have arranged for you to receive a complimentary one-year membership to Experian's® IdentityWorks™ credit monitoring service. This product helps detect possible misuse of your information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks™ is completely free to you, and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks™, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in this letter.

What We Are Doing.

From the moment we became aware of the incident, we worked closely with law enforcement and cybersecurity professionals. We regret that this occurred and apologize for any inconvenience. To help prevent something like this from happening again, we have taken steps to enhance our existing security measures.

IN THE CIRCUIT COURT OF THE FIRST CIRCUIT

STATE OF HAWAI‘I

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

Plaintiffs,

v.

HAWAIIUSA FEDERAL CREDIT UNION,

Defendant.

Case No.

DEMAND FOR JURY TRIAL

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the putative Class, demand a trial by jury on all issues so triable.

DATED: Honolulu, Hawai‘i January 30, 2024.

Respectfully Submitted,

/s/ Robert M. Hatch

Margery S. Bronster

Robert M. Hatch

Noelle E. Chan

BRONSTER FUJICHAKU ROBBINS

Gary M. Klinger (*pro hac vice* anticipated)

MILBERG COLEMAN BRYSON

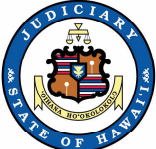

PHILLIPS GROSSMAN PLLC

Nickolas J. Hagman (*pro hac vice* anticipated)

CAFFERTY CLOBES MERIWETHER &

SPRENGEL LLP

Attorneys for Plaintiffs and the Proposed Class

STATE OF HAWAII CIRCUIT COURT OF THE FIRST CIRCUIT	SUMMONS TO ANSWER CIVIL COMPLAINT	CASE NUMBER
PLAINTIFF JOSEPH SMITH and TONY LEE, individually, and on behalf of all others similarly situated,	VS.	DEFENDANT(S) HAWAIIUSA FEDERAL CREDIT UNION,
PLAINTIFF'S NAME & ADDRESS, TEL. NO. Margery S. Bronster #4750/Robert M. Hatch #7724 Noelle E. Chan #11280 1003 Bishop Street, Suite 2300 Honolulu, Hawaii 96813 Telephone: (808) 524-5644		
<p>TO THE ABOVE-NAMED DEFENDANT(S)</p> <p>You are hereby summoned and required to file with the court and serve upon</p> <p>Margery S. Bronster/Robert M. Hatch 1003 Bishop Street, Suite 2300 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>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.</p> <p>A FAILURE TO OBEY THIS SUMMONS MAY RESULT IN AN ENTRY OF DEFAULT AND DEFAULT JUDGMENT AGAINST THE DISOBEYING PERSON OR PARTY.</p>		
The original document is filed in the Judiciary's electronic case management system which is accessible via eCourt Kokua at: http://www.courts.state.hi.us	<p>Effective Date of 28-Oct-2019 Signed by: /s/ Patsy Nakamoto Clerk, 1st Circuit, State of Hawaii</p> 	
 <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>		