STATE OF NEW MEXICO
COUNTY OF BERNALILLO
SECOND JUDICIAL DISTRICT COURT

BRENDA BRISCOE, individually and on behalf of all others similarly situated, Plaintiff, v. FIRST FINANCIAL CREDIT UNION, Defendant.	Case No. D-202-CV-2022-02974 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Brenda Briscoe ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through her attorneys, brings this Class Action Complaint against Defendant First Financial Credit Union ("FFCU"), and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against FFCU for its failure to secure and safeguard her and approximately 229,748 other individuals' private and confidential personally identifiable information ("PII"), including names, addresses, Social Security numbers, driver's license or government ID numbers, financial account information, and credit or debit card information.

2. FFCU is a New Mexico credit union with its principal place of business in Albuquerque, New Mexico and has locations throughout New Mexico.

3. Between January 17, 2022 and February 6, 2022, unauthorized individuals gained access to FFCU's network systems and accessed and acquired files from the system that contained the PII of Plaintiff and Class members (the "Data Breach").

4. FFCU owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. FFCU breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its members' and former members' PII from unauthorized access and disclosure.

5. As a result of FFCU's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all New Mexico residents whose PII was exposed as a result of the Data Breach, which FFCU first publicly acknowledged on or about April 7, 2022.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of express contract, breach of implied contract, unjust enrichment, and violation of the New Mexico Unfair Trade Practices Act, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Brenda Briscoe is a New Mexico resident. She provided her PII to FFCU in connection with receiving financial services. Had Plaintiff known that FFCU does not adequately protect PII, she would not have used FFCU's services and would not have agreed to provide FFCU with her PII. Despite Defendant's statement that all current and past members of the credit union were being notified of the breach, Plaintiff Briscoe has still yet to receive a notice regarding the data breach from FFCU.

8. Defendant First Financial Credit Union is a credit union created in New Mexico pursuant to the Credit Union Act, NMSA § 58-11-1, *et seq*., and has its principal place of business in Albuquerque, New Mexico. FFCU's corporate headquarters are located at 4910 Union Way NE, Albuquerque, NM 87107.

JURISDICTION AND VENUE

9. This Court has jurisdiction over the parties and the subject matter of this action because Defendant is a resident of New Mexico and was formed under te laws of New Mexico.

10. Venue is proper in Bernalillo County pursuant to NMSA 1978 § 38-3-1 because FFCU's principal place of business is located in Bernalillo County.

FACTUAL ALLEGATIONS

Overview of FFCU

11. FFCU is a credit union that was formed in 1937 and "serves the employees of over 200 companies."[1] The company has sixteen locations throughout New Mexico.[2]

12. In the regular course of its business, FFCU collects and maintains the PII of members and former members, and other persons to whom it is currently providing or previously provided services.

13. FFCU has a Privacy Policy that is provided to its members and is posted on its website. The Privacy Policy states, "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings."[3]

---

[1] *History*, First Financial Credit Union, https://www.ffnm.org/about/about-first-financial-credit-union/history.html (last accessed May 26, 2022).

[2] *Locations & Hours*, First Financial Credit Union, https://www.ffnm.org/about/get-in-touch/locations-hours.html (last accessed May 26, 2022).

[3] *Privacy Policy*, First Financial Credit Union, https://cms.bancvue.com/custom/fi/firstfinancialcu/fb/disclosure/privacy-policy.pdf (last

14. Plaintiff and Class members are, or were, customers of FFCU or received insurance or other services from FFCU, and entrusted FFCU with their PII.

The Data Breach

15. Between January 17, 2022 and February 6, 2022, an unauthorized individual, or unauthorized individuals, gained access to FFCU's network systems and accessed and acquired certain files on FFCU's computer systems.

16. FFCU did not begin to notify government agencies or the public directly about the Data Breach until two months after the Data Breach, on or about April 7, 2022. The notice that FFCU posted to its website states that the information that the cybercriminal extracted from FFCU's network includes an individual's "name, address, Social Security number, driver's license or government ID number, financial account information, and credit and/or debit card information."[4]

17. Cybercriminals claimed to have extracted the files from FFCU's computer systems and were threatening to post the information on the dark web, on a site known as LockBit 2.0.[5] The cybercriminals claimed to have 500 gigabytes of FFCU's data.[6] FFCU's CEO and president confirmed that FFCU was looking into the claims.[7] However, FFCU's notice makes no mention that the Data Breach was a ransomware attack or that cybercriminals extracted the files from FFCU's network systems.

FFCU Knew that Criminals Target PII

accessed May 26, 2022).
[4] Notice of Data Security Incident, FIRST FINANCIAL CREDIT UNION, https://www.ffnm.org/%20notice-of-data-security-incident.html (last accessed May 25, 2022).
[5] Chris Keller, *New Mexico Credit Union Investigating Claims Made By Known Ransomware Provider*, ALBUQUERQUE BUSINESS FIRST (March 10, 2022), https://www.bizjournals.com/albuquerque/news/2022/03/10/new-mexico-credit-union-ransomware-claims.html.
[6] *Id*.
[7] *Id*.

18. At all relevant times, FFCU knew, or should have known, its members', former members', Plaintiff's, and all other Class members' PII was a target for malicious actors. Despite such knowledge, FFCU failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that FFCU should have anticipated and guarded against.

19. PII is a valuable property right.[8] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[9] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[10] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

20. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims.

---

[8] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[9] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD iLIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[10] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

21. Consumers place a high value on the privacy of that data. Researchers have shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[11]

22. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

23. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[12]

24. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[13] According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives

---

[11] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

[12] *See* Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed May 26, 2022).

[13] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. 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. *Id*.

bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[14]

25. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[15]

26. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

27. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[16]

28. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it

---

[14] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (Sept. 1, 2017), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[15] Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), https://www.idtheftcenter.org/identity-theft-aftermath-study/ (last accessed May 26, 2022).

[16] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

takes approximately three months for consumers to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[17]

29. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

30. Plaintiff and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

CLASS ALLEGATIONS

31. This action is brought and may be properly maintained as a class action pursuant to N.M.R. Civ. P. Dist. Ct. 1-023.

32. Plaintiff brings this action on behalf of herself and all other members of the following Class of similarly situated persons:

[17] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

> All New Mexico residents whose PII was accessed by unauthorized persons in the Data Breach, including all New Mexico residents who were sent a notice of the Data Breach.

33. Excluded from the Class is First Financial Credit Union and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

34. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

35. The members in the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. FFCU reported to the Maine Attorney General that approximately 229,748 individuals' information was exposed in the Data Breach.

36. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether FFCU had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII from unauthorized access and disclosure;

b. Whether FFCU failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII;

c. Whether an implied contract existed between Class members and FFCU providing that FFCU would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

d. Whether FFCU breached its duties to protect Plaintiff's and Class members' PII; and

e. Whether Plaintiff and all other members of the Class are entitled to damages and the measure of such damages and relief.

37. FFCU engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

38. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by FFCU, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

39. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that she has no interests adverse to, or that conflict with, the Class she seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

40. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against FFCU, so it would be impracticable for

Class members to individually seek redress from FFCU's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. 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.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

41. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

42. FFCU owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

43. FFCU knew the risks of collecting and storing Plaintiff's and Class members' PII and the importance of maintaining secure systems. FFCU knew of the many data breaches that targeted companies that stored PII, including itself, in recent years.

44. Given the nature of FFCU's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, FFCU should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

45. FFCU breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to it—including Plaintiff's and Class members' PII.

46. It was reasonably foreseeable to FFCU that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

47. But for FFCU's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

48. As a result of FFCU's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT II
NEGLIGENCE PER SE

49. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

50. FFCU's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as

interpreted by the FTC, the unfair act or practice by business, such as FFCU, of failing to employ reasonable measures to protect and secure PII.

51. FFCU violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and Class members' PII and not complying with applicable industry standards. FFCU's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

52. FFCU's violation of Section 5 of the FTCA constitutes negligence per se.

53. FFCU and Class members are within the class of persons that Section 5 of the FTCA was intended to protect.

54. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA weas intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Brach.

55. It was reasonably foreseeable to FFCU that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

56. The injury and harm that Plaintiff and Class members suffered was the direct and proximate result of FFCU's violations of Section 5 of the FTCA. Plaintiff and Class members

have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT III
BREACH OF FIDUCIARY DUTY

57. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

58. Plaintiff and Class members gave FFCU their PII in confidence, believing that FFCU would protect that information. Plaintiff and Class members would not have provided FFCU with this information had they known it would not be adequately protected. FFCU's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between FFCU and Plaintiff and Class members. In light of this relationship, FFCU must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

59. FFCU has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class members' PII, failing to comply with data security guidelines, and otherwise failing to safeguard Plaintiff's and Class members' PII that it collected.

60. As a direct and proximate result of FFCU's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in FFCU's possession; and (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach.

COUNT IV
BREACH OF EXPRESS CONTRACT

61. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

62. Plaintiff and Class members and FFCU entered into written agreements regarding the services that FFCU was to provide to Plaintiff and Class members. Plaintiff and Class members paid FFCU monies, directly or through an insurance carrier and provided FFCU with their PII as consideration for these agreements. FFCU's document entitled "Privacy Practices" is evidence that data security was a material term of these contracts.

63. Plaintiff and Class members complied with the express contract when they paid FFCU and provided their PII to FFCU.

64. FFCU breached its obligations under the contracts between itself and Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII.

65. FFCU's breach of the express contracts between itself, on the one hand, and Plaintiff and Class members, on the other hand directly caused the Data Breach.

66. Plaintiff and all other Class members were damaged by FFCU's breach of express contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT V
BREACH OF IMPLIED CONTRACT

67. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

68. In connection with receiving services from FFCU, Plaintiff and all other Class members entered into implied contracts with FFCU.

69. Pursuant to these implied contracts, Plaintiff and Class members provided FFCU with their PII in order for FFCU to service their loans, for which FFCU is compensated. In exchange, FFCU agreed to, among other things, and Plaintiff understood that FFCU would: (1) provide services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members PII in compliance with federal and state laws and regulations and industry standards.

70. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and FFCU, on the other hand. Indeed, FFCU was clear in its Privacy Policy, and Plaintiff understood, that FFCU supposedly respects and is committed to protecting customer privacy.

71. Had Plaintiff and Class members known that FFCU would not adequately protect its members' and former members' PII, they would not have provided FFCU with their PII.

72. Plaintiff and Class members performed their obligations under the implied contracts when they provided FFCU with their PII.

73. FFCU breached its obligations under their implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

74. FFCU's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

75. Plaintiff and all other Class members were damaged by FFCU's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft—risk justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and/or (vi) lost time and money incurred to

mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

COUNT VI
UNJUST ENRICHMENT

76. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

77. This claim is pleaded in the alternative to the breach of express and implied contract claims.

78. Plaintiff and Class members conferred a monetary benefit upon FFCU in the form of monies paid for services.

79. FFCU accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. FFCU also benefitted from the receipt of Plaintiff's and Class members' PII, as this was used to facilitate payment.

80. As a result of FFCU's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

81. FFCU should not be permitted to retain the money belonging to Plaintiff and Class members because FFCU failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

82. FFCU should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VII
VIOLATION OF THE NEW MEXICO UNFAIR TRADE PRACTICES ACT ("UPA")
NMSA 1978 § 57–12–1 et seq.

83. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

84. The UPA defines an "unfair or deceptive trade practice" as "an act specifically declared unlawful pursuant to the [UPA], a false or misleading oral or written statement, visual description or other representation of any kind knowingly made in connection with the sale, lease, rental or loan of goods or services or in the extension of credit or in the collection of debts by a person in the regular course of his trade or commerce, which may, tends to or does deceive or mislead any person." NMSA 1978 § 57-12-2(D).

85. FFCU, Plaintiff, and all members of the class are "person[s]" as defined in NMSA 1978 § 57-12-2(A).

86. FFCU's credit union services constitute "trade" or "commerce" as defined in NMSA 1978 § 57-12-2(C).

87. FFCU made representations to Plaintiff and the Class members that their information would remain confidential, particularly in its Privacy Policy.

88. FFCU violated the UPA through its failure to adequately safeguard and maintain Plaintiff and Class members' PII.

89. As a result of FFCU's above-described conduct, Plaintiff and the Class have suffered damages from the disclosure of their information to unauthorized individuals.

90. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of FFCU's violations of the UPA. Plaintiff and Class members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face.

91. Plaintiff, individually and for each member of the Class, seeks actual damages and attorneys' fees, litigation expenses and court costs.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her and the Class's favor and against FFCU as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's designated counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent FFCU from experiencing another data breach by adopting and

implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 27, 2022

Respectfully submitted,

/s/ _Mark Fine__
MARK FINE
mark@thefinelawfirm.com
THE FINE LAW FIRM
220 9th St. NW
Albuquerque, NM 87102
Tel: 505.889.3463
Fax: 505.242.2716

BEN BARNOW*
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL*
aparkhill@barnowlaw.com
RILEY W. PRINCE*
rprince@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Ste. 1630
Chicago, IL 60606
Tel: 312.621.2000
Fax: 312.641.5504

TINA WOLFSON*
twolfson@ahdootwolfson.com
ROBERT AHDOOT*
rahdoot@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Tel: 310.474.9111
Fax: 310.474.8585

ANDREW W. FERICH*
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: 310.474.9111
Fax: 310.474.8585

*pro hac vice forthcoming