IN THE CIRCUIT COURT OF THE NINETEENTH JUDICIAL CIRCUIT
LAKE COUNTY, ILLINOIS

SHARITA MEDINA and JOHN WILLIAMS, individually and on behalf of all others similarly situated, Plaintiffs, v. ABBOTT LABORATORIES EMPLOYEES CREDIT UNION, Defendant.	Case No. 2024LA00000830 CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Sharita Medina and John Williams ("Plaintiffs"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through their attorneys, bring this Class Action Complaint against Defendant Abbott Laboratories Employees Credit Union ("ALEC" or "Defendant"), and complain and allege upon personal knowledge as to themselves and information and belief as to all other matters.

INTRODUCTION

1. Plaintiffs bring this class action against ALEC for its failure to secure and safeguard their and approximately 36,044 other individuals' personally identifying information ("PII"), including names, addresses, Social Security numbers, dates of birth, driver's license or other government issued ID numbers, and financial account information.

2. ALEC is a credit union who serves current and former employees of healthcare companies Abbott Laboratories and AbbVie, Inc. and their family members.

3. On or about August 2, 2024, an unauthorized third party accessed ALEC's network systems through an employee's email account and obtained files containing the PII of Plaintiffs and approximately 36,044 other current and former customers of ALEC (the "Data Breach").

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

5. As a result of ALEC's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiffs' and Class members' PII was accessed and stolen. This action seeks to remedy these failings and their consequences. Plaintiffs bring this action on behalf of themselves and all persons whose PII was exposed as a result of the Data Breach, which occurred on or about August 2, 2024.

6. Plaintiffs, on behalf of themselves and all other Class members, assert claims for negligence, breach of implied contract, unjust enrichment, and violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Sharita Medina

7. Plaintiff Sharita Medina is a citizen of Illinois.

8. Plaintiff Medina is a customer of ALEC who uses ALEC for banking or other financial services. As a condition of receiving such services, ALEC required Plaintiff Medina to provide it with her PII.

9. Based on representations made by ALEC, Plaintiff Medina believed ALEC had implemented and maintained reasonable security and practices to protect her PII. With this belief in mind, Plaintiff Medina provided her PII to ALEC in connection with obtaining banking or financial services provided by ALEC.

10. Plaintiff Medina takes great care to protect her PII. Had Plaintiff Medina known that ALEC does not adequately protect the PII in its possession, she would not have obtained banking or financial services from ALEC or agreed to entrust it with her PII.

11. At all relevant times ALEC stored and maintained Plaintiff Medina's PII on its network systems, including those systems affected in the Data Breach. ALEC stored and maintained Plaintiff Medina's PII such that it was accessible in or through its employees' email accounts, including the account accessed in the Data Breach.

12. Plaintiff Medina received a letter from ALEC informing her that her PII was affected by the Data Breach.

13. As a result of the Data Breach, Plaintiff Medina has suffered from a large increase in spam calls since the Data Breach occurred. In an attempt to mitigate the stress and annoyance of the spam calls she receives as a result of the Data Breach, Plaintiff Medina spent time installing and activating a spam call blocker.

14. As a direct result of the Data Breach, Plaintiff Medina has suffered injury and damages including, *inter alia*, a substantially increased and imminent risk of identity theft or fraud;

the wrongful disclosure and loss of confidentiality of her highly sensitive PII; deprivation of the value of her PII; and overpayment for services that did not include adequate data security.

Plaintiff John Williams

15. Plaintiff John Williams is a citizen of Illinois.

16. Plaintiff Williams is a customer of ALEC who uses ALEC for banking or other financial services. As a condition of receiving such services, ALEC required Plaintiff Williams to provide it with his PII.

17. Based on representations made by ALEC, Plaintiff Williams believed ALEC had implemented and maintained reasonable security and practices to protect his PII. With this belief in mind, Plaintiff Williams provided his PII to ALEC in connection with obtaining banking or financial services provided by ALEC.

18. Plaintiff Williams takes great care to protect his PII. Had Plaintiff Williams known that ALEC does not adequately protect the PII in its possession, he would not have obtained banking or financial services from ALEC or agreed to entrust it with his PII.

19. At all relevant times ALEC stored and maintained Plaintiff Williams's PII on its network systems, including those systems affected in the Data Breach. ALEC stored and maintained Plaintiff Williams's PII such that it was accessible in or through its employees' email accounts, including the account accessed in the Data Breach.

20. Plaintiff Williams received a letter from ALEC informing him that his PII was affected by the Data Breach.

21. As a result of the Data Breach, Plaintiff Williams has suffered from a large increase in spam calls since the Data Breach occurred.

22. As a direct result of the Data Breach, Plaintiff Williams has suffered injury and damages including, *inter alia*, a substantially increased and imminent risk of identity theft or fraud; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Defendant Abbott Laboratories Employees Credit Union

23. Defendant Abbott Laboratories Employees Credit Union is an Illinois credit union with its principal place of business located at 325 Tri-State Parkway, Gurnee, Illinois 60031.

JURISDICTION AND VENUE

24. This Court has general personal jurisdiction over Defendant Abbott Laboratories Employees Credit Union pursuant to 735 ILCS 5/2-209 because Defendant is organized under the laws of this State and regularly does business or solicits business, engages in other persistent courses of conduct, and derives substantial revenue from services provided to individuals in Lake County and in the State of Illinois, and expects or should reasonably expect to be in court here.

25. This Court has subject matter jurisdiction over this matter pursuant to Ill. Const. 1970, art. VI, § 9.

26. Venue is proper in Lake County pursuant to 735 ILCS 5/2-101 because Defendant resides in this County, conducts its usual and customary business in this County, and because a substantial portion of the events complained of occurred in this County.

FACTUAL ALLEGATIONS

Overview of Abbott Laboratories Employees Credit Union

27. ALEC is a credit union that serves employees and retirees of Abbott Laboratories and AbbVie, Inc., family members of current employees, and family members of current ALEC

members.[1] Abbott Laboratories researches and manufactures a variety of healthcare products and services.[2] AbbVie, Inc. is a biopharmaceutical company.[3]

28. ALEC provides banking and other financial services to more than 31,000 individuals and has over $1 billion in assets.[4] Abbott has approximately nine service centers, which are located in Abbott Labs facilities.[5]

29. In the regular course of its business, ALEC collects and maintains the PII of its current and former customers. ALEC required Plaintiffs and Class members to provide their PII as a condition of receiving banking or financial services from ALEC.

30. ALEC represents itself as "a financial institution that truly cares about you."[6] It states, "we exist solely to serve the diverse financial needs of our members," which is "an important distinction from many other financial institutions."[7] ALEC claims it delivers services with "honesty and sincerity" and that its customers "can depend on ALEC to work hard earning your trust."[8]

31. ALEC promises its customers that "[p]rotecting personal information and using it in a manner that is consistent with your expectations is a high priority for everyone associated with

---

[1] *About ALEC*, ALECU, https://www.alecu.org/membership/membership-benefits/about-alec (last accessed Nov. 1, 2024).
[2] *Abbott Laboratories*, BLOOMBERG, https://www.bloomberg.com/profile/company/ABT:US (last accessed Nov. 1, 2024).
[3] *AbbVie*, FORBES, https://www.forbes.com/companies/abbvie/ (last accessed Nov. 1, 2024).
[4] *About ALEC*, *supra* note 1.
[5] *Locations & ATMs*, ALECU, https://www.alecu.org/contact-us/locations-atms (last accessed Nov. 1, 2024).
[6] *About ALEC*, *supra* note 1.
[7] *Id.*
[8] *Id.*

ALEC."[9] ALEC claims it is "working hard to provide you with identity and security protection for you and your accounts."[10]

32. ALEC's website contains a privacy policy (the "Privacy Policy") that describes how ALEC collects, shares, and protects its customers' personal information.[11]

33. In the Privacy Policy, ALEC admits that as a financial company it "need[s] to share customers' personal information to run [its] everyday business."[12] It also admits that financial companies "choose how they share your personal information."[13] The Privacy Policy describes the reasons ALEC collects and shares its customers' PII, including for business and marketing purposes.[14]

34. In the Privacy Policy, ALEC promises that "[t]o 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."[15] ALEC additionally promises, "We also maintain other physical, electronic and procedural safeguards to protect this information, and we limit access to information to those employees for whom access is appropriate."[16]

---

[9] *ALEC Privacy Policy*, ALECU, https://www.alecu.org/membership/about/privacy-policy (last accessed Nov. 1, 2024).
[10] *Identity and Security Protection*, ALECU, https://www.alecu.org/membership/membership-benefits/identity-security-protection (last accessed Nov. 1, 2024).
[11] *What Does Alec Do With Your Personal Information?*, ALECU (Dec. 2017), https://assets.alecu.org/production/uploads/pdfs/Privacy-Notice-Disclosure.pdf?dm=1702328224 [hereinafter, the "*Privacy Policy*"].
[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.*

35. ALEC claims it continues to follow the practices and promises outlined in the Privacy Policy for the PII of persons who are no longer its customers.[17]

36. ALEC represents that is has "always believed there's no such thing as being too safe."[18] It promises its customers that, "Since our inception, protecting your account security and personal privacy has been a top priority."[19] It goes on to claim, "Today, we remain as committed as ever to updating our systems with the leading technologies to help keep your financial information safe from criminals who are eager to steal it."[20]

37. ALEC tells its customers, "Rest assured, your ALEC accounts are protected."[21] It claims it "employs highly advanced security procedures and very strict precautions."[22] ALEC further claims its "experienced staff continually monitor . . . our internal systems for any signs of fraud or criminal attempts to steal money or personal and sensitive information."[23]

38. ALEC's website describes a "host of high-level security precautions" it claims to utilize to protect its customers' PII, including:

a. Firewall. "ALEC's computer systems are protected 24/7 by a powerful firewall that blocks unauthorized entry. In order to gain access to authorized information, your web browser must know the proper protocol, or language — and even then, only select information is available."[24]

b. Encryption. "From the moment account information leaves your computer to the time it enters ALEC's system, all Online Banking sessions are

---

[17] *Id.*
[18] *How ALEC Protects You*, ALECU, https://www.alecu.org/membership/membership-benefits/how-alec-protects-you (last accessed Nov. 1, 2024).
[19] *Id.*
[20] *Id.*
[21] *Fraud and Scams*, ALECU, https://www.alecu.org/membership/membership-benefits/fraud-and-scams (last accessed Nov. 1, 2024).
[22] *Id.*
[23] *Id.*
[24] *How ALEC Protects You*, *supra* note 18.

encrypted. ALEC employs some of the strongest forms of encryption commercially available for use on the web today."[25]

c. Ongoing Monitoring. "ALEC carefully maintains and monitors our security systems constantly to provide maximum protection for your accounts."[26]

d. Technology Updates. "To address evolving online threats, ALEC has continued to enhance our security measures to help protect your accounts."[27]

39. ALEC acknowledges that "[t]he electronic world we live in is overflowing with potential security risks," and that "you and your personal data could be vulnerable to attack."[28]

40. ALEC is aware that "[i]dentity theft is one of the bad consequences of the world of electronic networking. When new openings appear, there is always a dishonest person looking to exploit it for fast, easy, robust gain."[29]

41. ALEC admits that:

> The easiest and probably most lucrative of all the scams being used today involves identity theft. Thieves only have to find out your key information to start an attack. Armed with your information, the thief could fraudulently buy goods, withdraw money from accounts, file taxes or get medical services. . . . Thieves will also use stolen information to open accounts online. With stolen credit card numbers, they can make purchases or advance money from accounts before the victim, the merchant, or the financial institution is aware that it's gone.[30]

42. ALEC recommends individuals take certain measures to prevent identity theft or fraud, and states that by following its guidelines "your security will be much harder to compromise."[31] ALEC's recommendations include, among other things, creating intricate

---

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] *Protecting Yourself Against ID Theft*, ALECU, https://www.alecu.org/membership/membership-benefits/protecting-against-id-theft (last accessed Nov. 1, 2024).
[29] *Id.*
[30] *Id.*
[31] *Id.*

passwords because "[c]omputers in the hands of thieves can zip through volumes of possible passwords in moments. Don't make it easy for them. . . . Using different passwords for each account limits fraudsters from accessing multiple accounts."[32] ALEC tells its customers not to give out their Social Security numbers.[33]

43. ALEC is aware of the harmful nature of spam calls, and knows that these calls can lead to fraud or identity theft. For this reason, ALEC recommends that its customers not respond to unsolicited calls and avoid giving out personal information over the phone.[34]

44. ALEC knows that "Electronic interaction between people in the worlds of commerce, industry, banking, entertainment, and everything else provides resourceful thieves unlimited opportunities to intrude and steal in the comfort of their living rooms. Your personal information, your money, your communications — just about everything about you — is available to resourceful crooks who can prey on the unwary computer user."[35]

45. ALEC advises its customers to, among other things, use complex passwords and do not reuse passwords because failing to do so "could enable hackers to gain entry into your other accounts as well," "Install a filter designed to ensure that the emails that get into your computer don't intend you any malice," "Use anti-malware and antivirus programs," and "Be especially wary of unsecured Wi-Fi sites. Save sensitive transactions for home, office, or places where you know your computer is protected."[36] ALEC further warns to be careful of suspicious emails or emails asking for sensitive or personal information.[37]

---

[32] *Id.*
[33] *Id.*
[34] *See id.*
[35] *Maintaining Computer Security*, ALECU, https://www.alecu.org/membership/membership-benefits/maintain-computer-security (last accessed Nov. 1, 2024).
[36] *Id.*
[37] *See id.*

46. ALEC admits that "institutions across the globe continue to report dramatic surges in fraudulent activity."[38] It is aware of the dangers of the increased risk of fraud and identity theft Plaintiffs and Class members now face because it knows "[h]aving access to your personal information is like money in the bank for criminals."[39] It warns its customers there "are a lot of scammers and fraudsters ready to take your money or your identity."[40]

47. ALEC recommends that persons whose personal information is compromised, including the PII affected in the Data Breach, "immediately" take action to prevent identity theft.[41] ALEC is aware that once PII is compromised, identity theft can go "undetected for years."[42]

48. Plaintiffs and Class members are current or former customers of ALEC and entrusted ALEC with their PII.

The Data Breach

49. On or about August 2, 2024, an unauthorized third party gained access to the email account of at least one ALEC employee.[43] According to the Notice Letter, the unauthorized third party "acquired certain information contained in the account," including the PII of Plaintiffs and Class members.[44] While ALEC has not publicly disclosed the specific information stolen in the Data Breach, the Texas Attorney General's Office reports the types of information affected includes "Name of individual; Address; Social Security Number Information; Driver's License

---

[38] *Fraud and Scams*, *supra* note 21.
[39] *Id.*
[40] *Id.*
[41] *How to Report Identity Theft*, ALECU, https://www.alecu.org/membership/membership-benefits/reporting-id-theft (last accessed Nov. 1, 2024).
[42] *Protecting Yourself Against ID Theft*, *supra* note 28.
[43] *ALEC Data Breach Notice Letter*, OFF. OF THE ME. ATT'Y GEN. (Oct. 18, 2024), available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/97df69a6-a63c-4640-8c0d-b480bc3807a0.html [hereinafter, the "*Notice Letter*"].
[44] *See id.*

number; Government-issued ID number (e.g. passport, state ID card); Financial Information (e.g. account number, credit or debit card number); [and] Date of Birth."[45]

50. ALEC did not discover the Data Breach until September 23, 2024, over seven weeks after the Data Breach occurred.[46] ALEC then waited another three weeks, until October 18, 2024—over two-and-a-half months after the Data Breach—to begin notifying its customers that their PII had been acquired by unauthorized persons.[47]

51. ALEC's failure to promptly notify Plaintiffs and Class members that their PII was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII 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.

ALEC Knew that Criminals Target PII

52. At all relevant times, ALEC knew, or should have known, that the PII it collects, shares, and maintains was a target for malicious actors. Despite such knowledge, ALEC failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class members' PII from unauthorized access and theft that ALEC should have anticipated and guarded against.

53. It is well known among companies that store sensitive PII that such information—such as the PII stolen in the Data Breach—is valuable and frequently targeted by criminals. In a

---

[45] *Data Security Breach Reports*, TEX. ATT'Y GEN. OFF. (Oct. 22, 2024), https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage

[46] *See Notice Letter*, *supra* note 43.

[47] *Id.*

recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[48]

54. PII is a valuable property right.[49] "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."[50] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[51] 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.

55. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security Numbers, 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 readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

---

[48] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[49] *See* Marc van Lieshout, *The Value of Personal Data*, 457 INT'L FED'N FOR INFO. 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.

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

[51] 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*, INTERACTIVE ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

56. Consumers place a high value on the privacy of their data, as they should. Researchers 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."[52]

57. 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.

58. It is no secret that "[b]usiness email hacking is a serious risk to businesses of all sizes and industries."[53] Unauthorized access to a employees' email account can cause numerous harms, including a data breach.[54] The compromise of a business's email account could cause employees and customers to "[f]ace widespread identity theft if personally identifiable information is stolen."[55]

59. Unauthorized access to an employee's email account is often intended to steal information.[56] "Attackers often target PII for identity theft or financial fraud."[57] Attackers who

---

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

[53] Travelers, *How to Protect Your Company from Business Email Compromise*, TRAVELERS, https://www.travelers.com/resources/business-topics/cyber-security/inside-an-email-hack (last accessed Nov. 1, 2024).

[54] *See id.*

[55] *What is business email compromise (BEC)?*, MICROSOFT, https://www.microsoft.com/en-us/security/business/security-101/what-is-business-email-compromise-bec (last accessed Nov. 1, 2024).

[56] *What Is Email Account Compromise (EAC)?*, PROOFPOINT, https://www.proofpoint.com/us/threat-reference/email-account-compromise (last accessed Nov. 1, 2024).

[57] *What is Data Theft?*, PROOFPOINT, https://www.proofpoint.com/us/threat-reference/data-theft (last accessed Nov. 1, 2024).

gain accessed to financial information "can use this information for financial gain, such as making unauthorized purchases or accessing bank accounts."[58]

60. Once an employee's email account has been compromised, the risk of harm remains ongoing because the attackers can "maintain access by creating email forwarding rules or changing account permissions, so they can closely monitor the victim and study the business."[59] Once an unauthorized person has access to a customer's information, that information can be used for "targeted phishing attacks or identity theft."[60]

61. To avoid the compromise of sensitive information in business or employee email accounts, experts recommend companies institute security measures such as encryption, system and network monitoring procedures, use of multifactor authentication, and conducting regular security audits.[61]

Theft of PII Has Grave and Lasting Consequences for Victims

62. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and

---

[58] *Id.*
[59] *What Is Email Account Compromise (EAC)?*, *supra* note 56.
[60] *What is Data Theft?*, *supra* note 57.
[61] *E.g.*, *id.*; *Business Email Compromise: What It Is and How to Prevent It*, STAY SAFE ONLINE (Dec. 18, 2023); https://staysafeonline.org/resources/business-email-compromise-what-it-is-and-how-to-prevent-it/#:~:text=In%20conducting%20a%20BEC%20attack,like%20their%20name%20and%20position.

incur charges and credit in a person's name.[62] [63] Unauthorized access to and theft of PII can cause individuals to face identity theft, monetary losses, privacy violations, and reputational damages.[64]

63. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[65]

64. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft. [66]

65. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately

---

[62] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Nov. 1, 2024).

[63] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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." 12 C.F.R. § 1022.3(g).

[64] *What is Data Theft?*, *supra* note 57.

[65] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[66] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Nov. 1, 2024).

three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[67]

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

Damages Sustained by Plaintiffs and the Other Class Members

67. Plaintiffs and all other Class members have suffered injury and damages, including, but not limited to: (i) a substantial increase in the likelihood of identity theft or fraud; (ii) the compromise, unauthorized access, 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 ALEC's possession; (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; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

68. This action is brought and may be properly maintained as a class action pursuant to 735 ILCS 5/2–801 *et seq.*

69. Plaintiffs bring this action on behalf of themselves and all members of the following Class of similarly situated persons:

---

[67] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

All persons whose PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all who were sent a notice of the Data Breach.

70. Excluded from the Class are Abbott Laboratories Employees 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.

71. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their 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.

72. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. ALEC has reported to the Maine Attorney General's Office that 36,044 persons were affected by the Data Breach.[68]

73. 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*:

e. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class members' PII from unauthorized access and disclosure;

f. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class members to unauthorized third parties;

g. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class members' PII;

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

[68] *See Notice Letter*, *supra* note 43.

i. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class members;

j. Whether Defendant breached its duties to protect Plaintiffs' and Class members' PII; and

k. Whether Plaintiffs and Class members are entitled to damages and the measure of such damages and relief.

74. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves 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.

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

76. Plaintiffs will fairly and adequately protect the interests of the Class members. Plaintiffs are adequate representatives of the Class in that they have no interests adverse to, or that conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

77. 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 Plaintiffs and Class members are relatively small compared to the burden and expense that would be required

to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant'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

78. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

79. ALEC owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting the PII in its possession, custody, or control.

80. ALEC knew or should have known the risks of collecting and storing Plaintiffs' and all other Class members' PII and the importance of maintaining secure systems. ALEC knew or should have known of the many data breaches and hacking attacks that targeted companies that collect and store PII in recent years.

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

82. ALEC'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 ALEC, of failing to employ reasonable measures to protect and secure PII.

83. ALEC's duties also arise from the Illinois Personal Information Protection Act ("IPIPA"), 815 ILCS 530/45(a), which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS. 530/45.

84. Additionally, under 815 ILCS 530/10, ALEC had a duty to "notify the resident at no charge that there has been a breach of the security of the system data following discovery or notification of the breach . . . in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10,

85. ALEC violated Section 5 of the FTCA and IPIPA by failing to use reasonable measures to protect Plaintiffs' and other Class members' PII, by failing to provide timely notice, and by not complying with applicable industry standards. ALEC'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 Plaintiffs and the other Class members.

86. ALEC's violation of its duties under, *inter alia*, common law, IPIPA, and Section 5 of the FTCA constitutes negligence.

87. Plaintiffs and Class members are within the class of persons that IPIPA and Section 5 of the FTCA were intended to protect.

88. The harm occurring as a result of the Data Breach is the type of harm that IPIPA and Section 5 of the FTCA were 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 Plaintiffs and Class members as a result of the Data Brach.

89. ALEC breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII.

90. It was reasonably foreseeable to ALEC that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' 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 Plaintiffs' and Class members' PII to unauthorized individuals.

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

92. As a result of ALEC's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs 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, unauthorized access, 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 ALEC's possession; (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; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
BREACH OF IMPLIED CONTRACT

93. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

94. In connection with receiving financial services, Plaintiffs and all other Class members entered into implied contracts with ALEC.

95. Pursuant to these implied contracts, Plaintiffs and Class members provided monies to ALEC to create financial accounts or in connection with financial services and provided ALEC with their PII. In exchange, ALEC agreed to, among other things, and Plaintiffs and ALEC understood that ALEC would: (1) provide services to Plaintiffs and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' PII; and (3) protect Plaintiffs' and Class members' PII in compliance with federal and state laws and regulations and industry standards.

96. The protection of PII was a material term of the implied contracts between Plaintiffs and Class members, on the one hand, and ALEC, on the other hand. Indeed, as set forth *supra*, ALEC recognizes the importance of data security and the privacy of its customers' PII, and repeatedly promises and represents that it protects its customers' PII. Had Plaintiffs and Class members known that ALEC would not adequately protect its customers' PII, they would not have received banking or other financial services from ALEC or agreed to provide ALEC with their PII.

97. Plaintiffs and Class members performed their obligations under the implied contract when they provided ALEC with their PII and paid for banking or other financial services from ALEC.

98. ALEC breached its obligations under its implied contracts with Plaintiffs 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 Plaintiffs' and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards.

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

100. Plaintiffs and all other Class members were damaged by ALEC's breach of implied contracts because: (i) they paid for banking or financial services that included reasonable and adequate data security measures, but did not receive the services they paid for; (ii) they face a substantially increased risk of identity theft—risks 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; (vi) they 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; and (vii) they paid for data security services the did not receive.

COUNT III
UNJUST ENRICHMENT

101. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

102. This claim is pleaded in the alternative to the breach of implied contract claim.

103. Plaintiffs and Class members conferred a monetary benefit upon ALEC by creating a financial account with ALEC, paying for banking or other financial services, and through the provision of their PII.

104. ALEC accepted or had knowledge of the benefits conferred upon it by Plaintiffs and Class members. ALEC also benefitted from the receipt of Plaintiffs' and Class members' PII, as this was used to facilitate services.

105. As a result of ALEC's conduct, Plaintiffs 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 Plaintiffs and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

106. It would be unjust to allow ALEC to retain the money belonging to Plaintiffs and Class members because ALEC failed to adequately implement the data privacy and security procedures for itself that Plaintiffs and Class members paid for, that ALEC promised to provide, and that were otherwise mandated by federal, state, and local laws and industry standards.

107. Plaintiffs and Class members have no adequate remedy at law.

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

COUNT IV
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/2, *et seq.* ("ICFA")

109. Plaintiffs reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

110. ALEC offered and continues to offer financial services in the State of Illinois.

111. Plaintiffs and Class members purchased and received banking or other financial services from ALEC for personal, family, or household purposes.

112. ALEC engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security measures to protect and secure its customers' PII in a manner that complied with applicable laws, regulations, and industry standards.

113. ALEC makes explicit statements to its customers that it implements measures to protect their PII, and that their PII will remain private.

114. ALEC's duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. ALEC violated this duty by failing to implement reasonably secure data security policies.

115. ALEC further violated the ICFA by failing to notify its current and former customers of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10.

116. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

117. Due to the Data Breach, Plaintiffs and Class members have lost property in the form of their PII. Further, ALEC's failure to adopt reasonable practices in protecting and safeguarding its customers' PII has forced, and will continue to force, Plaintiffs and Class members to spend time or money to protect against identity theft. Plaintiffs and Class members now face a substantially increased risk of identity theft, fraud, and other crimes. This harm sufficiently outweighs any justifications or motives for ALEC's practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information in place.

118. As a result of ALEC's violations of the ICFA, Plaintiffs and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft or fraud; (ii) the compromise, unauthorized access, 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 ALEC's possession; (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; and (vii) overpayment for the services that were received without adequate data security.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in their favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiffs as Class Representatives, and appointing Plaintiffs' counsel as Class Counsel;

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

C. Awarding Plaintiffs and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the Class, seek appropriate injunctive relief designed to prevent Defendant 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 and fraud;

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

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

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Class Action Complaint so triable.

Dated: November 4, 2024

Respectfully submitted,

/s/ Ben Barnow
Ben Barnow (IL Bar No. 0118265)
Anthony L. Parkhill (IL Bar No. 6317680)
Riley W. Prince (IL Bar No. 6339536)
Nicholas W. Blue (IL Bar No. 6343317)
BARNOW AND ASSOCIATES, P.C.
Cook County Attorney No. 38957

205 West Randolph Street, Suite 1630
Chicago, IL 60606
Tel: 312-621-2000
Fax: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com
rprince@barnowlaw.com
nblue@barnowlaw.com