IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF OKLAHOMA

1) LARRY LYLES on behalf of himself and all others similarly situated, Plaintiff, v. 2) AMERICAN BANK SYSTEMS, INC., Defendant.	)	Case No. CIV-21-23-HE

CLASS ACTION COMPLAINT

Plaintiff Larry Lyles ("Plaintiff"), brings this Class Action Complaint, on behalf of himself and all others similarly situated (the "Class"), against Defendant**,** American Bank Systems, Inc. ("ABS" or "Defendant"), alleging as follows based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to him, which are based on personal knowledge:

NATURE OF THE CASE

1. Plaintiff brings this class action against ABS for its failure to properly secure and safeguard Plaintiff's and the Class' highly-sensitive, protected personally identifiable information, including without limitation, names, dates of birth, phone numbers, addresses, bank account and loan information, and social security numbers (collectively, "PII"), for failing to comply with industry standards to protect information systems that contain PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had been compromised.

2. In November 2020, Avaddon, a group claiming to be the source of the attack published a "leak warning" claiming that they had successfully hacked into ABS's information systems and collected over 50 gigabytes of data from ABS and its customers (the "Data Breach"). The information contained highly-sensitive PII of ABS's customers. The group demanded a ransom in exchange for release of the data, coupled with a threat of public disclosure. According to certain published reports, Avaddon previously published the 4 GB portion of the database, threatening to publish more in the case ABS did not pay the requested fee. It appears that when ABS did not pay the fee, Avaddon published a 52.57 GB dump of the remaining data. Much of the data that was disclosed appears to have been stored by ABS in unencrypted, plain-text files – meaning that anyone who gained access to the files could fully read the information (and sensitive PII) therein.

3. Plaintiff seeks, among other things, damages, orders requiring ABS to fully and accurately disclose the nature of the information that has been compromised and to adopt reasonably sufficient security practices and safeguards to prevent incidents like the disclosure in the future, and for ABS to provide identity theft protective services to Plaintiff and Class Members for their lifetimes, as Plaintiff and Class Members will be at an increased risk of identity theft due to the conduct of ABS described herein.

4. ABS is a third-party vendor that provides compliance and document management solutions services to over 350 financial institutions in 35 states, which financial institutions serve many customers across the United States.

5. In the course of doing business with ABS, financial institutions implement ABS's software on their systems. In turn, ABS maintains credentialing information for financial

institutions, and ABS comes into possession of files containing the PII of financial institutions' customers and members.

6. One of ABS's financial institution customers, Missouri-based Freedom Bank of Southern Missouri ("Freedom"), used ABS to store information of its banking customers, including Plaintiff's information. On December 10, 2020, ABS notified Freedom's customers, including Plaintiff, that their PII that had been stored on ABS's systems was exfiltrated by unauthorized third parties. An exemplar of the Data Breach notification is attached hereto as "Exhibit A."

7. Since the Data Breach, ABS and its financial institution clients have issued similar notices, indicating that their customers also had PII compromised in the wide-reaching Data Breach.

8. As a result of ABS's failure to implement and follow basic security procedures, Plaintiff's and Class Members' PII is now in the hands of criminals. Plaintiff and Class Members face a substantial increased risk of identity theft, both currently and for the indefinite future. Consequently, Plaintiff and Class Members have had to spend, and will continue to spend, significant time and money in the future to protect themselves due to ABS's failures.

9. Plaintiff, on behalf of himself and all others similarly situated, alleges claims for violations of the Oklahoma Consumer Protection Act, negligence, negligence *per se*, unjust enrichment, and declaratory judgment. Plaintiff seeks damages and injunctive relief, including the adoption of reasonably sufficient practices to safeguard PII that remains in ABS's custody in order to prevent incidents like the Data Breach from reoccurring in the future.

PARTIES

10. Plaintiff Larry Lyles is a citizen and resident of the State of Arkansas. At all times relevant to this Complaint, Plaintiff's PII was stored with ABS. His PII was disclosed without authorization to unknown third parties as a result of the ABS Data Breach.

11. Plaintiff received a letter from ABS stating that they experienced a data security incident and unauthorized third parties were able to view and acquire data from ABS containing his PII.

12. Since the announcement of the Data Breach, Plaintiff has been required to spend his valuable time monitoring his various accounts in an effort to detect and prevent any misuses of his PII – time which he would not have had to expend but for the Data Breach.

13. As a result of the Data Breach, Plaintiff will continue to be at heightened risk for fraud and identity theft, and their attendant damages for years to come.

14. Defendant American Bank Systems, Inc. is an Oklahoma corporation that provides document management and compliance software solutions to the financial services industry. Defendant's registered address for service of process is 14000 Parkway Commons Drive, Oklahoma City, OK, 73134, and its principal place of business is at the same location.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interests and costs.

16. This Court has personal jurisdiction over Defendant because it maintains its principal place of business in this District. Further, at all relevant times it has engaged in substantial business activities, including the sale of financial systems management services, in this State. Defendant has, at all relevant times, transacted, solicited, and conducted business in this State through its employees, agents, and/or sales representatives, and derived substantial revenue from such business in this State.

17. Pursuant to 28 U.S.C. § 1391(b)(1), venue is proper in this District because Defendant resides in this District and is a resident of the state in which this District is located.

FACTUAL BACKGROUND

American Bank Systems

18. ABS markets itself as having "created advanced management systems for the financial industry that help assess, monitor and lower compliance risk"[1] and being "[t]he bank systems software suite most trusted by banking professionals."[2]

19. ABS represents that it "help[s] financial institutions operate efficiently and confidently in a rapidly evolving – highly regulated – environment. As a leading provider of bank and compliance systems specifically designed for the financial industry, American Bank System has created a suite of banking software that streamlines bank processes, eliminates compliance headaches and solves document imagining challenges." [3]

20. ABS's software product offerings include BankManager, CreditUnionPro, CompliancePro, and CoPilot Loans and Deposits. These programs perform a variety of functions,

[1] https://www.americanbanksystems.com/about/
[2] https://www.americanbanksystems.com/banking-systems/
[3] https://www.americanbanksystems.com

including streamlining lending processes through document tracking and storage management, linking customer accounts and data across multiple systems, report generation, compliance monitoring, and other similar services.

21. Defendant currently "is serving more than 350 banks, credit unions and other financial institutions in 35 states – and counting."[4]

22. As part of its relationship with financial institutions, ABS routinely acquires and stores the financial institutions' customers' PII on its systems. Financial institutions save time and money by using ABS's services by not having to pay the cost of in-house compliance personnel or maintaining the systems and infrastructure required of a dedicated server.

23. In the course of doing business with ABS, financial institutions implement ABS's software on their systems. In turn, ABS maintains credentialing information for financial institutions, and ABS comes into possession of files containing the PII of financial institutions' customers and members.

24. Financial institution customers demand security to safeguard their PII. As a vendor storing sensitive financial related data, ABS is required to ensure that such private, sensitive information is not disclosed or disseminated to unauthorized third parties.

Background on Ransomware Attacks and Avaddon

25. Ransomware is a well-known and increasingly common form of cyberattack in which the attacker introduces malware to the target's systems. The malware then uses encryption methods to block the victim from using or accessing the targeted system or data.

26. The malware is typically introduced to the victim's systems through a relatively unsophisticated route: malicious "Trojan" emails sent to specific users who have access to the

[4] https://www.americanbanksystems.com/about/

target's systems. The emails include attachments disguised as ordinary excel files, jpegs, or zip drives, or links that appear to be for package tracking or other innocent purposes. If the user opens the malicious attachment or clicks the link and allows it to download an application, a program will open that either unpacks the ransomware directly or allows the attackers gain a foothold in the system to launch further attacks.

27. Once the ransomware is in place, the malware typically includes instructions for contacting the attacker, who then offers to remove the malware or provide a decryption key in exchange for payment, often in the form of Bitcoin or another cryptocurrency. In some instances, referred to by some as "double extortion," the attacker also exfiltrates sensitive data and threatens to release it to the public, or sell it on the "dark web," if the ransom demands are not met.

28. The number of ransomware attacks increased dramatically during the 2010s, and some well-known variants, such as WannaCry, Locky, and Petya, have been used in thousands of separate attack incidents. Targets have included all sizes of businesses in virtually every sector, non-profits including hospitals and universities, and government agencies.

29. Beginning in or around July 2020, a cybercrime news publication described a new variant of ransomware called Avaddon.[5] The report identified that the typical delivery route was, like most other malware attacks, a Trojan email with a malicious attachment, with subject lines suggesting that the attachment contained a photograph of the recipient.[6]

30. The news report also described how the malicious file unloads the ransomware to the user's system, which system folders are targeted for encryption, and alterations the ransomware

[5] Trend Micro, *Ransomware Report: Avaddon and New Techniques Emerge, Industrial Sector Targeted*, July 8, 2020 (updated July 23, 2020), available at: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-report-avaddon-and-new-techniques-emerge-industrial-sector-targeted

[6] *Id.*

makes to running Windows processes and services.[7] The article also included examples of a desktop image the ransomware places on the user's computer which points the user to the "ransom note," which in turn describes how the victim can contact the attackers in order to "buy" a decryption program.[8]

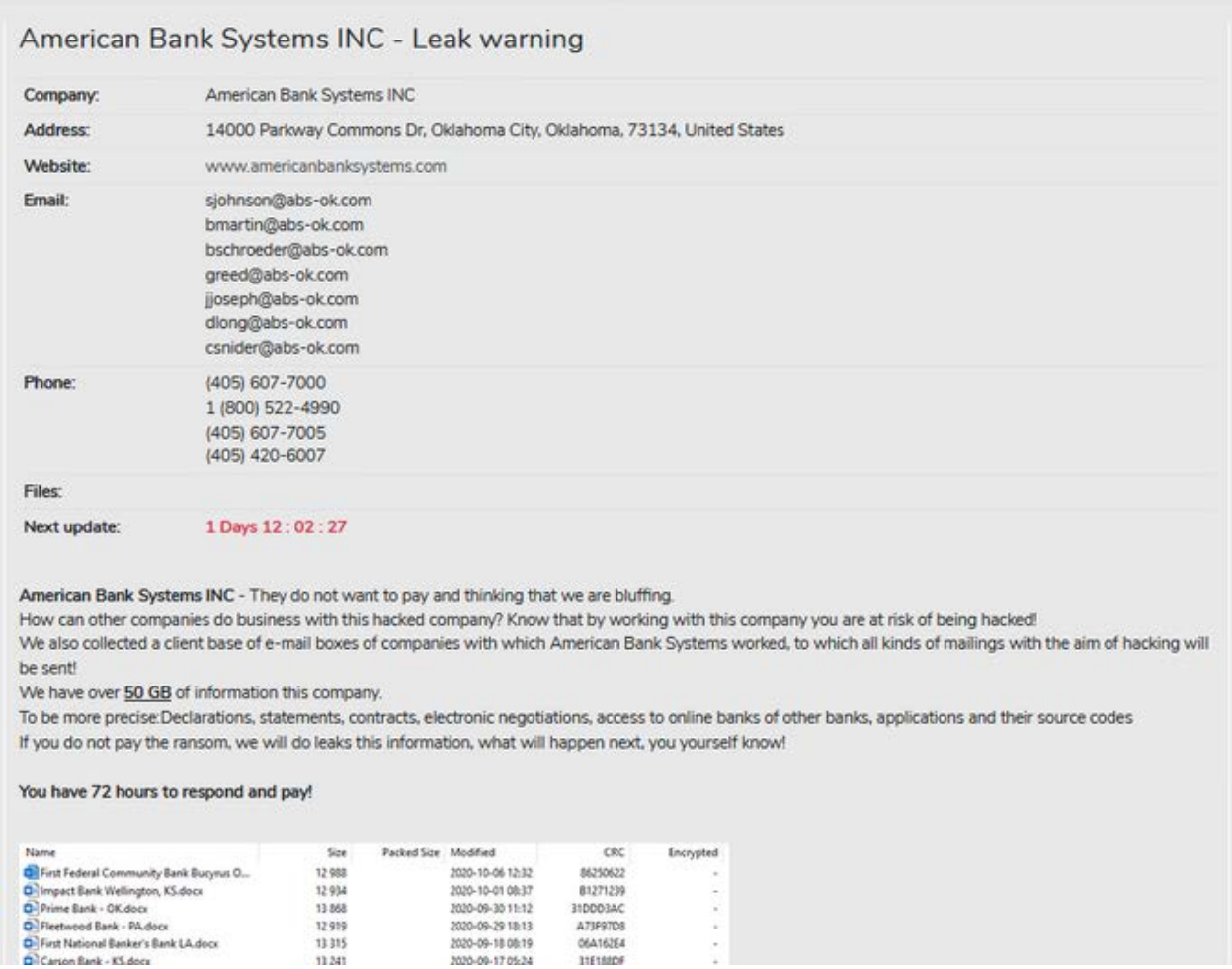
31. Another data security blog reported in August 2020 that the operators of Avaddon set up their own website on which to publish leaked data whenever a victim failed to pay ransom.[9]

The ABS Data Breach

32. In early November 2020, the group purporting to be behind the Avaddon malware attacks published a "leak warning" claiming that they had hacked ABS and taken possession of over 50 gigabytes of data. The group demanded a ransom in exchange for release of the data, coupled with a threat of public disclosure.[10]

33. Avaddon posted that ABS "do[es] not want to pay and think[] that we are bluffing." The group contemporaneously leaked four gigabytes of the stolen data.[11]

[7] *Id.*
[8] *Id.*
[9] https://cofense.com/avaddon-ransomware-joins-data-exfiltration-trend/
[10] https://securityreport.com/american-bank-systems-hit-by-ransomware-attack-full-53-gb-data-dump-leaked/?web_view=true
[11] *Id.*



American Bank Systems INC - Leak warning

Company:	American Bank Systems INC
Address:	14000 Parkway Commons Dr, Oklahoma City, Oklahoma, 73134, United States
Website:	www.americanbanksystems.com
Email:	sjohnson@abs-ok.com bmartin@abs-ok.com bschroeder@abs-ok.com greed@abs-ok.com jjoseph@abs-ok.com dlong@abs-ok.com csnider@abs-ok.com
Phone:	(405) 607-7000 1 (800) 522-4990 (405) 607-7005 (405) 420-6007
Files:	
Next update:	1 Days 12 : 02 : 27

American Bank Systems INC - They do not want to pay and thinking that we are bluffing.
How can other companies do business with this hacked company? Know that by working with this company you are at risk of being hacked!
We also collected a client base of e-mail boxes of companies with which American Bank Systems worked, to which all kinds of mailings with the aim of hacking will be sent!
We have over **50 GB** of information this company.
To be more precise:Declarations, statements, contracts, electronic negotiations, access to online banks of other banks, applications and their source codes
If you do not pay the ransom, we will do leaks this information, what will happen next, you yourself know!

You have 72 hours to respond and pay!

Name	Size	Packed Size	Modified	CRC	Encrypted
First Federal Community Bank Bucyrus O...	12 988		2020-10-06 12:32	86250622	-
Impact Bank Wellington, KS.docx	12 934		2020-10-01 08:37	B1271239	-
Prime Bank - OK.docx	13 868		2020-09-30 11:12	31D0D3AC	-
Fleetwood Bank - PA.docx	12 919		2020-09-29 10:13	A73F97D8	-
First National Banker's Bank LA.docx	13 315		2020-09-18 08:19	06A162E4	-
Carson Bank - KS.docx	13 241		2020-09-17 05:24	31E188DF	-

34. Analysis by one news outlet indicated that the sample leak included a variety of highly sensitive information, such as loan documents, login credentials for financial institutions' internal file sharing networks, and financial records. In turn, some of the leaked financial documents included banking customers' PII, including names, social security numbers, loan amounts, interest rates, and pertinent loan dates such as origination dates, maturity dates, and pay off dates. Astonishingly, much of this sensitive data appears to have been stored by ABS in unencrypted, plaintext files – meaning that anyone who gained access to the files could fully read the information (and sensitive PII) therein.[12]

[12] *Id.*

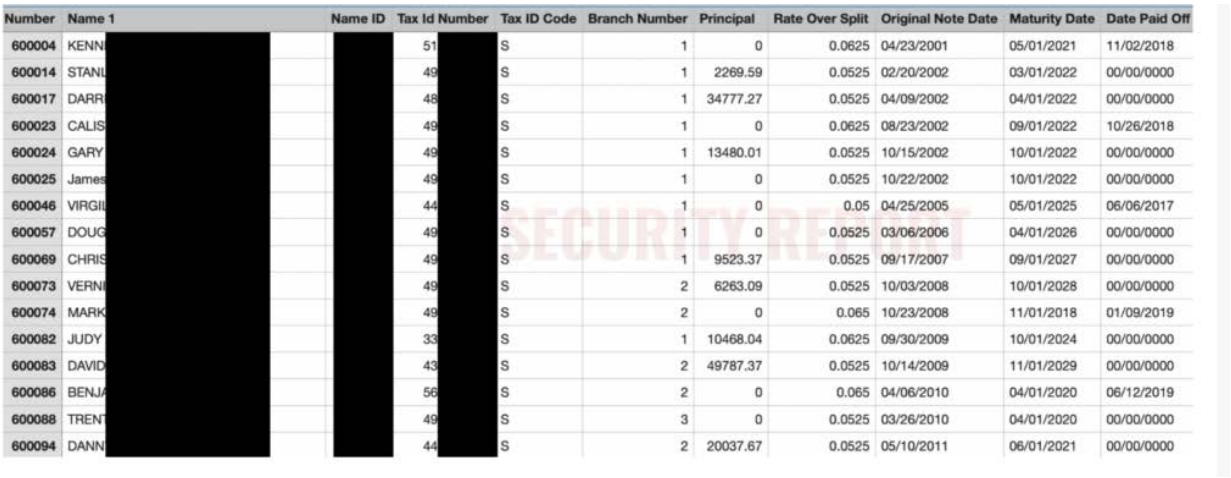
35. Avaddon posted a screenshot of some of the data that was obtained from ABS[13]:

Name	Size	Packed Size	Modified	CRC	Encrypted
First Federal Community Bank Bucyrus O...	12 988		2020-10-06 12:32	86250622	-
Impact Bank Wellington, KS.docx	12 934		2020-10-01 08:37	B1271239	-
Prime Bank - OK.docx	13 868		2020-09-30 11:12	31DDD3AC	-
Fleetwood Bank - PA.docx	12 919		2020-09-29 18:13	A73F97D8	-
First National Banker's Bank LA.docx	13 315		2020-09-18 08:19	06A162E4	-
Carson Bank - KS.docx	13 241		2020-09-17 05:24	31E188DF	-
Merchants And Farmers Bank Leesville LA....	13 385		2020-09-10 10:54	DDC85086	-
First State Bank Waynesboro MS.docx	13 364		2020-08-20 13:11	E40020E5	-
InFirst Bank Indiana PA.docx	13 408		2020-08-18 12:50	4A3C10AB	-
First National Bank And Trust Of Okmulge...	12 616		2020-08-14 10:00	83C46900	-
Farmers and Merchants National Bank Fair...	14 273		2020-07-20 10:13	ED3D11AB	-
Citizens Bank of Americus Americus GA.d...	13 013		2020-07-15 10:46	A054EE10	-
Unico Bank Mineral Point MO.docx	13 987		2020-07-08 13:35	761A7C48	-
22nd State Bank Louisville AL.docx	13 396	563 400	2020-07-06 08:44	3D60ECAB	-
The Tri-County Bank NE.docx	13 097		2020-06-29 06:15	FAEC4365	-
Prairie Bank of Kansas Stafford KS.docx	13 749		2020-06-05 11:06	81796BB7	-
The Farmers State Bank McPherson - KS.d...	12 934		2020-06-05 07:35	973977CA	-
First National Bank in Cimarron KS.docx	14 185		2020-06-04 07:46	0E2935E7	-
Community National Bank Okarche OK.do...	13 736		2020-05-28 11:14	E22ECD17	-
The Bank Of New Madrid - MO.docx	13 088		2020-05-27 06:57	C2BAA89B	-
Table Rock Community Bank Kimberling C...	12 883		2020-05-19 07:44	1D068B10	-
Royal Bank Elroy WI.docx	14 018		2020-05-15 14:12	8C4A96D2	-
SNB Shattuck OK.docx	13 999		2020-04-15 07:45	D8C1E925	-
Bank Of Commerce Catoosa - OK.docx	14 524		2020-03-24 10:28	7277C6FC	-
First National Bank Pulaski TN.docx	15 454		2020-03-23 06:34	C157A170	-
Peoples Exchange Bank Monroeville AL.do...	13 360		2020-03-11 10:25	80F4E631	-
AllNations Bank Calumet OK.docx	13 606		2020-03-10 07:31	0851AA93	-
First Bank and Trust of Memphis TX.docx	12 898		2020-03-03 09:22	0B94A1DC	-

36. Avaddon also posted a screenshot of the PII, such as customers' names, Tax ID numbers (likely Social Security Numbers), and loans from ABS, that was exposed by this breach.

[13] *Id.*

14



Number	Name 1	Name ID	Tax Id Number	Tax ID Code	Branch Number	Principal	Rate Over Split	Original Note Date	Maturity Date	Date Paid Off
600004	KENN[redacted]	[redacted]	51[redacted]	S	1	0	0.0625	04/23/2001	05/01/2021	11/02/2018
600014	STANL[redacted]	[redacted]	49[redacted]	S	1	2269.59	0.0525	02/20/2002	03/01/2022	00/00/0000
600017	DARR[redacted]	[redacted]	48[redacted]	S	1	34777.27	0.0525	04/09/2002	04/01/2022	00/00/0000
600023	CALIS[redacted]	[redacted]	49[redacted]	S	1	0	0.0625	08/23/2002	09/01/2022	10/26/2018
600024	GARY[redacted]	[redacted]	49[redacted]	S	1	13480.01	0.0525	10/15/2002	10/01/2022	00/00/0000
600025	James[redacted]	[redacted]	49[redacted]	S	1	0	0.0525	10/22/2002	10/01/2022	00/00/0000
600046	VIRGI[redacted]	[redacted]	44[redacted]	S	1	0	0.05	04/25/2005	05/01/2025	06/06/2017
600057	DOUG[redacted]	[redacted]	49[redacted]	S	1	0	0.0525	03/06/2006	04/01/2026	00/00/0000
600069	CHRIS[redacted]	[redacted]	49[redacted]	S	1	9523.37	0.0525	09/17/2007	09/01/2027	00/00/0000
600073	VERN[redacted]	[redacted]	49[redacted]	S	2	6263.09	0.0525	10/03/2008	10/01/2028	00/00/0000
600074	MARK[redacted]	[redacted]	49[redacted]	S	2	0	0.065	10/23/2008	11/01/2018	01/09/2019
600082	JUDY[redacted]	[redacted]	33[redacted]	S	1	10468.04	0.0625	09/30/2009	10/01/2024	00/00/0000
600083	DAVID[redacted]	[redacted]	43[redacted]	S	2	49787.37	0.0525	10/14/2009	11/01/2029	00/00/0000
600086	BENJ[redacted]	[redacted]	56[redacted]	S	2	0	0.065	04/06/2010	04/01/2020	06/12/2019
600088	TRENT[redacted]	[redacted]	49[redacted]	S	3	0	0.0525	03/26/2010	04/01/2020	00/00/0000
600094	DANN[redacted]	[redacted]	44[redacted]	S	2	20037.67	0.0525	05/10/2011	06/01/2021	00/00/0000

37. The article indicated that, based on timestamps on screenshots of the leaked files, the breach initially began "sometime in or before early October."[15]

38. ABS indicated in its letter to Plaintiff that it learned of the Data Breach on October 22, 2020.

39. ABS apparently did not pay the ransom, and by November 14, 2020 the full 52.57 gigabytes of stolen data, including Plaintiff's and the Class Members' PII, in the Avaddon group's possession was leaked.[16]

40. According to ABS, it notified Freedom of the Data Breach on November 2, 2020, which was approximately 10 days after ABS reported it learned of the incident, and did not notify Plaintiff until more than a month later on December 10, 2020.

[14] *Id.*

[15] *Id.*

[16] *Id.*

Financial Information is Particularly Vulnerable to Data Breaches

41. ABS, a company that promotes its trustworthiness, has a responsibility to securely maintain the customer PII that it receives and keep it safe from harm. ABS was on notice that PII, specifically when it includes financial information, is a prime target for data breaches.

42. "Due to the nature of these businesses and the sensitivity of their data, financial firms are hit with approximately 300 times more cyber attacks than businesses in other industries."[17]

43. "In 2018 the sector reported 819 cyber incidents, a significant increase from the 69 incidents report in 2017."[18]

44. "Banks and financial services organizations were the targets of 25.7 percent of all malware attacks last year, more than any other industry."[19]

45. Particularly during Covid-19, while employees are working remotely, cybercriminals are working to exploit fear and uncertainty. From February to April 2020, cyber attacks in the financial sector increased by 238 percent.[20]

46. ABS knew, or should have known, the importance of safeguarding Plaintiff's and Class Members' PII entrusted to it by financial institutions around the country and knew, or should have known, the foreseeable consequences if that data was disclosed. This includes the significant costs that would be imposed on users as a result of a breach. ABS failed, however, to take adequate

[17] https://www.bitsight.com/blog/financial-data-breaches-2019-capital-one-first-american-desjardins-more
[18] *Id.*
[19] https://www.forbes.com/sites/zakdoffman/2019/04/29/new-cyber-report-25-of-all-malware-hits-financial-services-card-fraud-up-200/?sh=a15e9e17a47a
[20] https://www.helpnetsecurity.com/2020/06/17/cybercriminals-sophisticated/

cybersecurity measures to prevent the Data Breach from occurring.

ABS Obtains, Collects, and Stores Plaintiff's and Class Members' PII

47. In the ordinary course of doing business with ABS's customers—financial institutions—Plaintiff and Class Members are regularly required to provide their sensitive, personal and private protected information in order to open accounts, obtain loans, and perform other financial activities.

48. Due to ABS's role as a third-party vendor for financial institutions, Plaintiff and Class Members have no direct contractual relationship with ABS, and were generally unaware that ABS had access to Plaintiff and Class Members' PII.

49. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, ABS assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

50. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and they reasonably expect that vendors who work with their financial institutions will use the utmost care to keep this information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

51. ABS acknowledges the seriousness of protecting personal information. As stated in Defendant's Privacy Policy:

> We take our users' privacy very seriously. We feel that certain personal information should always be kept private. We have technology measures to protect any personal information you submit from misuse and loss, such as firewalls and password-protected areas using established industry standards. These measures are also designed to protect personal information from unauthorized access, modification, and disclosure. However, no data protection measures

> are entirely foolproof when data is transmitted and stored over the Internet.

52. Despite Defendant's commitment to protecting personal information, ABS failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiff's and Class Members' PII.

53. Had ABS remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, ABS could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential PII.

The Value of Private Information and Effects of Unauthorized Disclosure

54. ABS was well aware that the protected financial information and PII it touches is highly sensitive and of significant value to those who would use it for wrongful purposes.

55. PII is a valuable commodity to identity thieves. As the Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and medical and financial fraud.[21] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII and other protected financial information on multiple underground Internet websites, commonly referred to as the "dark web."

56. While PII is valued at approximately $1 per line of information, "Bank account credentials can sell for anywhere between $200 and $500 apiece. . . ."[22]

[21] https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft
[22] https://www.master-solutions.com/blog/your-identity-can-sell-on-the-black-market-for-somewhere-between-1-500

57. Protected financial information is particularly valuable because criminals can use not only a person's personal information for identity theft, but can also gain access to bank accounts and cash contained therein.

58. "Financial identity theft is a significant crime, and potentially one of the more damaging types of identity theft. Consider the possibilities – an identity thief gaining access to your bank accounts or retirements accounts and stealing your hard-earned money."[23]

59. The ramifications of ABS's failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

60. Further, criminals often trade stolen PII on the "cyber black market" for years following a breach. Cybercriminals can also post stolen PII on the internet, thereby making such information publicly available.

61. ABS knew, or should have known, the importance of safeguarding the PII entrusted to it and of the foreseeable consequences if its data security systems were breached. ABS failed, however, to take adequate cyber security measures to prevent the Data Breach from occurring.

FTC Guidelines

62. ABS is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

[23] https://www.lifelock.com/learn-identity-theft-resources-what-is-financial-identity-theft.html

63. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[24]

64. The FTC provides cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understands their network's vulnerabilities, and implement policies to correct any security problems.[25]

65. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[26]

66. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

67. ABS failed to properly implement basic data security practices. ABS's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

---

[24] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf
[25] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136proteting-personal-information.pdf.
[26] *Id.*

68. ABS was at all times fully aware of its obligations to protect the PII of consumers because of its position as a compliance solutions provider for financial institutions, which gave it direct access to consumer PII. ABS was also aware of the significant repercussions that would result from its failure to do so.

Plaintiff and Class Members Suffered Damages

69. The ramifications of ABS's failure to keep PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud, occurring 65 percent of the time.[27]

70. In 2019 alone, consumers lost more than $1.9 billion to identity theft and fraud.[28]

71. Besides the monetary damage sustained, consumers may also spend anywhere from approximately 7 hours to upwards of 1,200 hours trying to resolve identity theft issues.[29]

72. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

73. Despite all of the publicly available knowledge of the continued compromises of PII, ABS's approach to maintaining the privacy of protected financial information and other PII was reckless, or in the very least, negligent.

---

[27] https://www.identityforce.com/blog/identity-theft-odds-identity-theft-statistics#:~:text=In%202019%2C%2014.4%20million%20consumers,about%201%20in%2015%20people&text=Identity%20theft%20is%20the%20most,data%20breaches%20increased%20by%2017%25

[28] *Id.*

[29] https://www.lifelock.com/learn-identity-theft-resources-how-long-does-it-take-to-recover-from-identity-theft.html#:~:text=And%20ID%20theft%20recovery%20is,more%20resolving%20identity%20theft%20problems.

74. As a result of ABS's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer injuries, including loss of time and productivity through efforts to ameliorate, mitigate, and deal with the future consequences of the Data Breach; theft of their valuable PII; the imminent and certain impeding injury flowing from fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII that was entrusted to Defendant with the understanding the Defendant would safeguard the PII against disclosure; and continued risk to Plaintiff's and the Class Members' PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate an adequate measures to protect the PII that was entrusted to it.

CLASS ALLEGATIONS

75. Plaintiff brings this case individually and, pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the class defined as:

> All individuals in the United States, and its territories, whose PII was compromised in the American Bank Systems Data Breach which occurred between October and November 2020.

76. Excluded from the Class is Defendant, its subsidiaries and affiliates, their officers, directors and members of their immediate families and any entity in which Defendant has a controlling interest, the legal representatives, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

77. Plaintiff reserves the right to modify or amend the definition of the proposed Class if necessary before this Court determines whether certification is appropriate.

78. The requirements of Rule 23(a)(1) are satisfied. The class described above is so numerous that joinder of all individual members in one action would be impracticable. The disposition of the individual claims of the respective class members through this class action will benefit both the parties and this Court. The exact size of the class and the identities of the individual members thereof are ascertainable through Defendant's records, including but not limited to, the files implicated in the Data Breach.

79. The requirements of Rule 23(a)(2) are satisfied. There is a well-defined community of interest and there are common questions of fact and law affecting members of the Class. The questions of fact and law common to the Class predominate over questions which may affect individual members and include the following:

a. Whether and to what extent Defendant violated the Oklahoma Consumer Protection Act;

b. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

c. Whether Defendant was negligent in collecting and storing Plaintiff's and Class Members' PII;

d. Whether Defendant had duties not to disclose the PII of Class Members to unauthorized third parties;

e. Whether Defendant took reasonable steps and measures to safeguard Plaintiff's and Class Members' PII;

f. Whether Defendant failed to adequately safeguard the PII of Class Members;

g. Whether Defendant breached its duties to exercise reasonable care in handling Plaintiff's and Class Members' PII by storing that information unencrypted on

computers and hard drives in the manner alleged herein, including failing to comply with industry standards;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant had respective duties not to use the PII of Class Members for non-business purposes;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

k. Whether Plaintiff and Class Members are entitled to damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

80. The requirements of Rule 23(a)(3) are satisfied. Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same failure by Defendant to safeguard PII.

81. Plaintiff and members of the Class were each customers of financial institutions that were clients of ABS, each having their PII obtained by an unauthorized third party.

82. The requirements of Rule 23(a)(4) are satisfied. Plaintiff is an adequate representative of the class because his interests do not conflict with the interests of the members of the Class. Plaintiff will fairly, adequately, and vigorously represent and protect the interests of

the members of the Class and has no interests antagonistic to the members of the Class. In addition, Plaintiff has retained counsel who are competent and experienced in the prosecution of class action litigation. The claims of Plaintiff and the Class members are substantially identical as explained above. While the aggregate damages that may be awarded to the members of the Class are likely to be substantial, the damages suffered by the individual members of the Class are relatively small. As a result, the expense and burden of individual litigation make it economically infeasible and procedurally impracticable for each member of the Class to individually seek redress for the wrongs done to them. Certifying the case as a Class will centralize these substantially identical claims in a single proceeding, which is the most manageable litigation method available to Plaintiff and the Class and will conserve the resources of the parties and the court system, while protecting the rights of each member of the Class. Defendant's uniform conduct is generally applicable to the Class as a whole, making relief appropriate with respect to each Class member.

FIRST CAUSE OF ACTION

VIOLATIONS OF OKLAHOMA CONSUMER PROTECTION ACT OKLA. STAT., TIT. 15, CH. 20 §§ 751, *et seq* (On Behalf of Plaintiff and the Class)

83. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

84. ABS is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

85. ABS offers, sells, and distributes goods, services, and other things of value which constitute "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

86. ABS, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753(8);

d. Committing unfair trade practices that offend established public policy and were immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

e. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

87. ABS's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures

following previous incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681e, and the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801, *et seq;*

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq*.

88. ABS's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of ABS's data security and ability to protect the confidentiality of consumers' PII.

89. ABS intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

90. Had ABS disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, ABS would not have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law.

91. Instead, ABS held itself out as having "created advanced management systems for the financial industry that help assess, monitor and lower compliance risk"[30] and being "[t]he bank systems software suite most trusted by banking professionals"[31] and that it serves more than 350 banks, credit unions and other financial institutions in 35 states – and counting.[32] This included PII from tens of thousands of consumers, including Plaintiff and the Class. ABS held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Plaintiff and the Class members acted reasonably in relying on ABS's misrepresentations and omissions, the truth of which they could not have discovered.

92. The above unlawful practices and acts by ABS were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Class members.

93. ABS acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff's and the Class members' rights.

94. As a direct and proximate result of ABS's unlawful practices, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses of money or

[30] https://www.americanbanksystems.com/about/
[31] https://www.americanbanksystems.com/banking-systems/
[32] https://www.americanbanksystems.com/about/

property, and monetary and non-monetary damages, including time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

95. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

SECOND CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

96. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

97. ABS owed a duty under common law to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their PII in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty including, among other things: (a) designing, maintaining, and testing ABS's security systems to ensure that Plaintiff's and Class Members' PII in ABS's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warning and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

98. ABS's duty to use reasonable care arose from several sources, including but not limited to those described below.

99. ABS had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of Defendant. By collecting and storing valuable PII that

is routinely targeted by criminals for unauthorized access, ABS was obligated to act with reasonable care to protect against these foreseeable threats.

100. ABS's duty also arose from ABS's position as a financial institution vendor. ABS undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers and consumers cannot "opt out" of ABS's data collection activities. ABS holds itself out as a trusted steward of consumer data, and thereby assumes a duty to reasonably protect that data. The consumer public have no choice but to repose a trust and confidence in ABS to perform that stewardship carefully. Otherwise consumers would be powerless to fully protect their interests with regard to their PII, which is controlled by ABS. Because of its crucial role within the financial system, ABS was in a unique and superior position to protect against the harm suffered by Plaintiff and Class Members as a result of the ABS Data Breach.

101. ABS admits that it has the responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the PII at issue here.

102. ABS breached the duties owed to Plaintiff and Class Members and thus was negligent. ABS breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiff and Class Members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiff's and Class Members' PII in ABS's possession had been or was reasonably believed to have been, stolen or compromised.

103. But for ABS's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their PII would not have been compromised.

104. As a direct and proximate result of ABS's negligence, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with requested credit freezes;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of the financial accounts;

d. Costs associated with purchasing credit monitoring and identity theft protection services;

e. Unauthorized charges and loss of use of and access to their financial account funds and costs associated with 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 of their credit;

f. Lowered credit scores resulting from credit inquiries following fraudulent activities;

g. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the ABS Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

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

i. Damages to and diminution in value of their PII entrusted, directly or indirectly, to ABS with the mutual understanding that ABS would safeguard Plaintiff's and Class Members data against theft and not allow access and misuse of their data by others; and

j. Continued risk of exposure to hackers and thieves of their PII, which remains in ABS's possession and is subject to further breaches so long as ABS fails to undertake appropriate and adequate measures to protected Plaintiff.

105. As a direct and proximate result of ABS's negligence, Plaintiff and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Class)

106. Plaintiff restates and realleges all preceding factual allegations above as if fully set forth herein.

107. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as ABS or failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of ABS's duty.

108. ABS violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with the industry standards. ABS's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach within the financial industry.

109. ABS's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

110. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

111. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and Class Members.

112. As a direct and proximate result of ABS's negligence, Plaintiffs and Class Members have been injured as described herein and in Paragraph 104 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

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

113. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

114. Plaintiff and Class Members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by ABS and that was ultimately stolen in the ABS Data Breach.

115. ABS was benefitted by the conferral upon it of the PII pertaining to Plaintiff and Class Members and by its ability to retain and use that information. ABS understood that it was in fact so benefitted.

116. ABS also understood and appreciated that the PII pertaining to Plaintiff and Class Members was private and confidential and its value depended upon ABS maintaining the privacy and confidentiality of that PII.

117. But for ABS's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with ABS. Further, if ABS had disclosed that its data security measures were inadequate, ABS would not have been permitted to continue in operation by regulators and participants in the marketplace.

118. As a result of ABS's wrongful conduct as alleged in this Complaint (including among other things its utter failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that PII), ABS has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

119. ABS's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identify thieves.

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

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

122. ABS is therefore liable to Plaintiff and Class Members for restitution in the amount of the benefit conferred on ABS as a result of its wrongful conduct, including specifically the value to ABS of the PII that was stolen in the ABS Data Breach and the profits ABS received from the use of that information.

FIFTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(On Behalf of Plaintiff and the Class)

123. Plaintiff restates and realleges all preceding allegations above as if fully set forth herein.

124. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

125. An actual controversy has arisen in the wake of the ABS Data Breach regarding Plaintiff's and Class Members' PII and whether ABS is currently maintaining data security measures adequate to protect Plaintiff's and Class Members from further data breaches that compromise their PII. Plaintiff alleges that ABS's data security measures remain inadequate. ABS denies these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his PII and remains at imminent risk that further compromises of his PII will occur in the future.

126. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

i. ABS owes a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

ii. ABS continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

127. This Court also should issue corresponding prospective injunctive relief requiring ABS to employ adequate security protocols consistent with law and industry standards to protect consumers' PII.

128. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at ABS. The risk of another such breach is real, immediate, and substantial. If another breach at ABS occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

129. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to ABS if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to ABS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and ABS has a pre-existing legal obligation to employ such measures.

130. Issuance of the requested injunction will not disserve the public interest. To the contract, such an injunction would benefit the public by preventing another data breach at ABS, thus eliminating the additional injuries that would result to Plaintiff and consumers whose confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE Plaintiff on behalf of himself and all other similarly situated, prays for relief as follows:

a. For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

b. For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

c. For damages in an amount to be determined by the trier of fact;

d. For an order of restitution and all other forms of equitable monetary relief;

e. Declaratory and injunctive relief as described herein;

f. Awarding Plaintiff's reasonable attorneys' fees, costs, and expenses;

g. Awarding pre- and post-judgment interest on any amounts awarded; and,

h. Awarding such other and further relief as may be just and proper.

JURY TRIAL DEMAND

A jury trial is demanded on all claims so triable.

Dated: January 11, 2021

Respectfully submitted,

/s/ William B. Federman

William B. Federman, OBA #2853
Molly E. Brantley, OBA #33126
Tyler J. Bean, OBA #33834
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
meb@federmanlaw.com
tjb@federmanlaw.com

/s/ Gary F. Lynch
Gary F. Lynch (PA ID 56887)*
Jamisen A. Etzel (PA ID 311554)*
Nicholas A. Colella*
CARLSON LYNCH, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
T: (412) 322-9243
F: (412) 231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com
ncolella@carlsonlynch.com

Counsel for Plaintiff

*Pro Hac Vice Forthcoming

JS 44 (Rev. 06/17)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

LARRY LYLES on behalf of himself and all others similarly situated,

(b) County of Residence of First Listed Plaintiff Carroll County, AR
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
William B. Federman -- FEDERMAN & SHERWOOD- 10205 N. Pennsylvania Ave., Okl. City, OK 73120 (405-235-1560)

DEFENDANTS

American Bank Systems, Inc.

County of Residence of First Listed Defendant Oklahoma County
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ❒ 1 U.S. Government Plaintiff
- ❒ 3 Federal Question *(U.S. Government Not a Party)*
- ❒ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	❒ 1	☒ 1	Incorporated *or* Principal Place of Business In This State	❒ 4	❒ 4
Citizen of Another State	☒ 2	❒ 2	Incorporated *and* Principal Place of Business In Another State	❒ 5	❒ 5
Citizen or Subject of a Foreign Country	❒ 3	❒ 3	Foreign Nation	❒ 6	❒ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
❒ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	❒ 625 Drug Related Seizure of Property 21 USC 881	❒ 422 Appeal 28 USC 158	❒ 375 False Claims Act
❒ 120 Marine	❒ 310 Airplane	❒ 365 Personal Injury - Product Liability	❒ 690 Other	❒ 423 Withdrawal 28 USC 157	❒ 376 Qui Tam (31 USC 3729(a))
❒ 130 Miller Act	❒ 315 Airplane Product Liability	❒ 367 Health Care/ Pharmaceutical Personal Injury Product Liability		PROPERTY RIGHTS	❒ 400 State Reapportionment
❒ 140 Negotiable Instrument	❒ 320 Assault, Libel & Slander	❒ 368 Asbestos Personal Injury Product Liability		❒ 820 Copyrights	❒ 410 Antitrust
❒ 150 Recovery of Overpayment & Enforcement of Judgment	❒ 330 Federal Employers' Liability	PERSONAL PROPERTY	LABOR	❒ 830 Patent	❒ 430 Banks and Banking
❒ 151 Medicare Act	❒ 340 Marine	❒ 370 Other Fraud	❒ 710 Fair Labor Standards Act	❒ 835 Patent - Abbreviated New Drug Application	❒ 450 Commerce
❒ 152 Recovery of Defaulted Student Loans (Excludes Veterans)	❒ 345 Marine Product Liability	❒ 371 Truth in Lending	❒ 720 Labor/Management Relations	❒ 840 Trademark	❒ 460 Deportation
❒ 153 Recovery of Overpayment of Veteran's Benefits	❒ 350 Motor Vehicle	☒ 380 Other Personal Property Damage	❒ 740 Railway Labor Act	SOCIAL SECURITY	❒ 470 Racketeer Influenced and Corrupt Organizations
❒ 160 Stockholders' Suits	❒ 355 Motor Vehicle Product Liability	❒ 385 Property Damage Product Liability	❒ 751 Family and Medical Leave Act	❒ 861 HIA (1395ff)	❒ 480 Consumer Credit
❒ 190 Other Contract	❒ 360 Other Personal Injury		❒ 790 Other Labor Litigation	❒ 862 Black Lung (923)	❒ 490 Cable/Sat TV
❒ 195 Contract Product Liability	❒ 362 Personal Injury - Medical Malpractice		❒ 791 Employee Retirement Income Security Act	❒ 863 DIWC/DIWW (405(g))	❒ 850 Securities/Commodities/ Exchange
❒ 196 Franchise				❒ 864 SSID Title XVI	❒ 890 Other Statutory Actions
				❒ 865 RSI (405(g))	❒ 891 Agricultural Acts
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	IMMIGRATION	FEDERAL TAX SUITS	❒ 893 Environmental Matters
❒ 210 Land Condemnation	❒ 440 Other Civil Rights	Habeas Corpus:	❒ 462 Naturalization Application	❒ 870 Taxes (U.S. Plaintiff or Defendant)	❒ 895 Freedom of Information Act
❒ 220 Foreclosure	❒ 441 Voting	❒ 463 Alien Detainee	❒ 465 Other Immigration Actions	❒ 871 IRS—Third Party 26 USC 7609	❒ 896 Arbitration
❒ 230 Rent Lease & Ejectment	❒ 442 Employment	❒ 510 Motions to Vacate Sentence			❒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
❒ 240 Torts to Land	❒ 443 Housing/ Accommodations	❒ 530 General			❒ 950 Constitutionality of State Statutes
❒ 245 Tort Product Liability	❒ 445 Amer. w/Disabilities - Employment	❒ 535 Death Penalty			
❒ 290 All Other Real Property	❒ 446 Amer. w/Disabilities - Other	Other:			
	❒ 448 Education	❒ 540 Mandamus & Other			
		❒ 550 Civil Rights			
		❒ 555 Prison Condition			
		❒ 560 Civil Detainee - Conditions of Confinement			

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ❒ 2 Removed from State Court ❒ 3 Remanded from Appellate Court ❒ 4 Reinstated or Reopened ❒ 5 Transferred from Another District *(specify)* ❒ 6 Multidistrict Litigation - Transfer ❒ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. §1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005

Brief description of cause:
Negligence due to theft of Personally Identifiable Information

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ❒ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE Charles B. Goodwin DOCKET NUMBER CIV-20-1307-G

DATE 01/11/2021

SIGNATURE OF ATTORNEY OF RECORD /s/ William B. Federman

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

Print Save As... Reset

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.