IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

Lynne Askew, *individually and on behalf of all others similarly situated*, Plaintiff, v. Gas South, LLC, Defendant.	**Case No.** 2022CV369337 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Lynne Askew, individually and on behalf of all others similarly situated, brings this action against Defendant Gas South, LLC ("Gas South" or "Defendant") to obtain damages, restitution, and injunctive relief for the Class, as defined below. Plaintiff makes the following allegations upon information and belief, except as to her own actions, the investigation of her counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. This class action arises out of a "data incident" perpetrated against Defendant Gas South, a natural gas company that provides natural gas services for customers in Georgia, as well as a handful of other states, that occurred between

February 13, 2022 and February 23, 2022 (the "Data Breach"). The Data Breach resulted in unauthorized access and exfiltration of highly sensitive and personal information.

2. As a result of the Data Breach, Plaintiff and approximately **38674**[1] putative class members ("Class") suffered present injury and damages in the form of identity theft, out-of-pocket expenses and the value of the time reasonably incurred to remedy or mitigate the effects of the unauthorized access, exfiltration, and subsequent criminal misuse of their sensitive and highly personal information.

3. The personal information compromised in the Data Breach included, *inter alia*, the full names and Social Security numbers of Gas South customers. The Data Breach likely includes other Personal Information that Gas South failed to list specifically or otherwise disclose to the public, Plaintiff, and Class members. Each Class Member received a belated notice of the Data Breach from Gas South ("Notice Letter").[2]

4. The specific data, which was compromised in Gas South's Data Breach, is highly sensitive, protected information that can and is likely to be used to commit identity theft against Class members. Plaintiff's and Class Members' Social Security numbers are deemed personally identifiable information ("PII").

[1] *See* Office of the Maine Attorney General, Data Breach Notifications, available at: https://apps.web.maine.gov/online/aeviewer/ME/40/976742a7-101d-4270-bc7f-fdbac4ed6ec5.shtml (last accessed August 23, 2022).
[2] *See, e.g.*, Plaintiff's Notice Letter, attached as Exhibit A.

5. Plaintiff brings this class action lawsuit on behalf of herself and those similarly situated to address Defendant's inadequate safeguarding of Class Members' Personal Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of a third party.

6. Upon information and belief, Defendant maintained the Personal Information in a reckless manner. As evidenced by the Data Breach, the Personal Information on Defendant's computer system and network was unencrypted and maintained in a condition vulnerable to cyberattacks.

7. The potential for a cyberattack and subsequent improper disclosure of Plaintiff's and Class Members' Personal Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Personal Information from the risk of a cyberattack.

8. Plaintiff's and Class Members' identities are now at considerable risk because of Defendant's negligent conduct since the PII that Gas South collected and maintained is now in the hands of data thieves.

9. Armed with the Personal Information accessed in the Data Breach, data thieves can commit a variety of crimes, including but not limited to fraudulently applying for unemployment benefits, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members'

names to obtain medical services, using Class Members' information to target other hacking intrusions based on their individual needs, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph and providing false information to police during an arrest.

10. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. As a result of Defendant's actions and inactions, as set forth herein, Plaintiff and Class Members must now and in the future closely monitor their financial accounts and information to guard against identity theft, among other issues.

11. Plaintiff and Class Members have and may in the future incur actual monetary costs, including but not limited to the cost of purchasing credit monitoring services, credit freezes, credit reports or other protective measures to deter and detect identity theft.

12. Plaintiff and Class Members have and will in the near future be required to expend time spent mitigating the effects of the Data Breach, including time spent dealing with actual or attempted fraud and identity theft.

13. By her Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data

Breach, identifiable by the list of individuals to whom Gas South has sent or has attempted to send a Notice Letter.

14. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long-term credit monitoring services funded by Defendant.

16. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserts claims for negligence, negligence per se, breach of implied contract, invasion of privacy, unjust enrichment, breach of confidence, and violations of the Georgia Uniform Deceptive Trade Practices Act.

PARTIES

17. Plaintiff Lynne Askew is, and at all times mentioned herein was, an individual citizen of the State of Georgia residing in the City of Stockbridge in Henry County.

18. Defendant Gas South, LLC is a Limited Liability Company established in 2005, pursuant to the laws of the State of Georgia. It provides natural gas services

for customers who are residents of Georgia. Gas South maintains its principal place of business at 3625 Cumberland Blvd, Suite 1500, Atlanta, Georgia, 30339. According to the Georgia Secretary of State's records, Gas South can be served through its registered agent, Jamie Tiernan, 3625 Cumberland Blvd, Suite 1500, Atlanta, GA, 30339.

JURISDICTION AND VENUE

19. This Court has personal jurisdiction over Defendant Gas South, LLC as it is a domestic limited liability company in good standing, organized under the laws of the State of Georgia, with its principal place of business in Atlanta (Fulton County), Georgia and a majority (if not all) of its business is in the State of Georgia, thus rendering the exercise of personal jurisdiction by this Court proper and necessary.

20. This Court has personal jurisdiction over Defendant Gas South, as the company has sufficient minimum contacts with the State of Georgia. Defendant Gas South intentionally avails itself of the markets within this district to render the exercise of jurisdiction by this court just and proper. Defendant Gas South does business in the State of Georgia (through, among other things, its service contract with class members) and the business being done in Georgia directly relates to the subject of this lawsuit, thus rendering the exercise of personal jurisdiction by this court proper and necessary.

21. Venue is proper because a substantial part of the events and omissions giving rise to these claims occurred in Atlanta, Fulton County, Georgia.

22. Upon information and belief, a federal district court would be forced to decline to exercise CAFA jurisdiction over this matter, if filed in the federal courts. Pursuant to 28 U.S.C. § 1332(d)(4)(B), and based upon Gas South's headquarters, its overwhelming presence and extensive business holdings in the State of Georgia, Plaintiff believes that "two-thirds or more of the members of all proposed plaintiff classes in the aggregate, and the primary defendants, are citizens of the State of Georgia." Alternatively, the local controversy exception, 28 U.S.C. § 1332(d)(4)(A), may apply as "during the 3-year period preceding the filing of that class action, no other class action has been filed asserting the same or similar factual allegations against any of the defendants."

FACTUAL ALLEGATIONS

Defendant's Business

23. Defendant Gas South provides natural gas to customers in Georgia, as well as in other states. Those services are provided to residential, industrial, wholesale, municipal, and business customers.[3] It provides moving services for customers who keep their gas service plans, and it also has three event venues.[4]

[3] *See* https://www.gassouth.com/gas-for-business (last accessed August 23, 2022).
[4] *See* https://www.gassouth.com/common/gas-south-district (last accessed August 23, 2022).

These venues accommodate concerts, performances, meetings, trade shows, conventions, banquets, and celebrations of large sizes.

24. As it conducts its business, Gas South collects highly sensitive PII from its customers. If any customer refuses to provide the required PII, upon information and belief, Gas South is unlikely to provide services to that customer.

25. In the ordinary course of doing business with Defendant, customers were required to provide (and Plaintiff and Class Members did in fact provide) Gas South with Personal Information such as:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Driver's license number;
- Photo identification;
- Employer information;
- Information obtained during customer visits; and
- Payment information.

26. Although Gas South claims in its Notice Letters that "[i]nformation privacy and security are among our highest priorities, and [it] has security measures in place to protect information in [its] care."[5]

27. Gas South does not follow its own policies or industry standard practices in securing customers' PII.

28. On information and belief, Gas South inadequately trains its employees on cybersecurity policies, fails to enforce those policies, or maintains unreasonable or inadequate security practices and systems.

The Data Breach

29. On or about February 21, 2022, Gas South discovered that it was the victim of what it refers to as "a data incident." In its "Notice of Security Incident" ("Notice"), posted online and similar to the Notice Letters received by Plaintiff and Class Members, "Upon identifying unusual activity on certain systems, Gas South disconnected these systems from the network and commenced an investigation."[6]

30. Defendant engaged in a "review of its systems" to determine the nature and scope of this incident and to "identify and populate address information for any potentially affected individuals."[7]

---

[5] *See* Plaintiff's Notice Letter, Exhibit A.
[6] Notice of Security Incident, available at: https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-397.pdf (last accessed August 23, 2022). *See also* Plaintiff's Notice Letter, Exhibit A.
[7] *Id.*

31. Defendant determined that an unauthorized person or people accessed Gas South's computer systems between February 13, 2022 and February 23, 2022, and at during that ***ten day period*****,** accesses a cache of highly sensitive Personal Information it had stored there, including names with associated Social Security numbers.

32. By July 15, 2022, ***about 5 months*** after the Class's Personal Information was first accessed by cybercriminals, Gas South finally began to notify customers that its investigation identified that their Personal Information was breached. Although Gas South has not divulged to Plaintiff, the Class, or the public the exact information that was accessed, upon information and belief it includes or may include: an individuals' name; address and other contact information; Social Security number, date of birth, and/or driver's license number (collectively, "PII").

33. Defendant explicitly admits that the PII of Plaintiff and Class Members was accessed by "an unknown actor" without authorization[8] and stated in its July 15, 2022 Notice letters that its investigation is not complete.

34. Defendant was aware of its data security obligations, and understands that those obligations are particularly important given the substantial increase in data breaches for businesses that collect and store PII preceding the date of the breach.

[8] *See* Exhibit A.

35. Cyberattacks, such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

36. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and the data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of cyber-attacks and data breaches;
b. Failing to adequately protect the Personal Information of its customers;
c. Failing to properly monitor its own data security systems for existing intrusions to enable it to quickly stop any attack and mitigate the harm;
d. Failing to ensure that vendors with access to Gas South's protected information data employed reasonable security procedures;
e. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,
f. Failing to adhere to industry standards for cybersecurity.

37. As the result of its inadequate security and procedures, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Personal Information.

38. In its Notice Letters to Plaintiff and the Class, Gas South admits that after the Data Breach it has begun "reviewing and enhancing [its] existing policies and procedures to reduce the likelihood of a similar future event."[9] These measures could have—and should have—been in place prior to the Data Breach, and likely could have prevented the Data Breach from occurring.

39. Despite its lag in notification of the Data Breach that affected customers, Gas South offered victims of the attack just 12 months of identity theft services through Experian Identity Works. These services include 12 months of monitoring, fraud consultation, and identity theft restoration.

40. Based on the Notice of Data Breach letter Plaintiff received, which informed Plaintiff that her Personal Information was "accessed"—and included her name and Social Security number, Plaintiff reasonably believes her Personal Information was intentionally accessed, stolen from Defendant's network in the Data Breach, and was sold on the Dark Web.

41. Further, the removal of the Personal Information from Defendant's system – information that included full names, dates of birth, and Social Security

[9] *See, e.g.,* Plaintiff's Notice Letter, attached as Exhibit A.

numbers (which are the keys to identity theft and fraud) demonstrates that this cyberattack was targeted.

42. Due to Defendant's insufficient security measures, Plaintiff and the Class Members now face an increased risk of fraud and identity theft and must deal with the risk the misuse of their Personal Information for years.

Defendant Failed to Comply with FTC Guidelines

43. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[10]

[10] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited August 23, 2022).

45. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[11]

46. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive 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.

47. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data (like the Personal Information in this matter), 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

48. Defendant failed to properly implement basic data security practices.

[11] *Id*.

49. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII of its customers constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

50. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

51. As noted above, experts studying cyber security routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

52. Several best practices have been identified that at a minimum should be implemented by businesses like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

53. Other best cybersecurity practices that are standard in the industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting

up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

55. Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Identity Theft is Costly for Victims

56. In 2007, the United States Government Accountability Office released a report regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good

name and credit record."[12] Its warnings and recommendations are even more applicable now as the incidence of identity theft rises each year.

57. Victims of a data breach are exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the data on the black market where other thieves take over victims' identities to engage in illegal financial transactions under the victims' names.

58. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

[12] *See* U.S. Gov. Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007). Available at https://www.gao.gov/new.items/d07737.pdf (last accessed August 23, 2022).

59. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit and correcting their credit reports.[13]

60. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud and bank/finance fraud.

61. PII is a valuable property right, and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Personal Information has considerable market value.

62. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when Personal Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold

[13] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited August 23, 2022).

> or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at 29.

63. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

64. There is a strong probability that entire batches of the Private Information taken from Gas South have been dumped on the black market and are yet to be dumped on the black market—including names and Social Security numbers—meaning Plaintiff and Class Members face a substantial and imminent risk of fraud and identity theft now and for many years into the future.

65. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts now and for many years to come.

66. Sensitive Personal Information can sell for as much as $363 per record according to the Infosec Institute.[14] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

[14] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last accessed August 23, 2022).

67. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[15] Such fraud may go undetected until debt collection calls commence months, or even years, later.

68. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[16]

69. Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

70. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are

[15] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed August 16, 2022).
[16] *Id.* at 4.

able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[17]

71. Data like a Social Security number, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security [n]umbers are worth more than 10x on the black market."[18]

Elderly Populations Are Reluctant to Change After a Data Breach

72. In 2020, the AARP sponsored Javelin Strategy Research to do a report on identity fraud strategies for Americans aged 55 years and older. While this report and its related research show that elders experience similar rates of being victims or identity fraud as the overall U.S. population, it also indicates certain troublesome patterns among this population.[19]

73. After being a victim of identity fraud, "[c]onsumers aged 65+ typically do not change how they shop, bank, or pay following a fraudulent event. A

[17] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed August 23, 2022)

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed August 23, 2022).

[19] Identity Fraud in Three Acts: A Consumer Guide, available at: https://www.aarp.org/content/dam/aarp/home-and-family/family-and-friends/2020/10/aarp-Identity-fraud-report.pdf, at 8 (last accessed August 23, 2022).

surprising 70% of consumers 65 and older exhibit reluctance to change familiar habits."[20] This reluctance increases the risks that elders face after a data breach like that at Gas South.

74. For Americans 55+ years old, Javelin's research has shown that they are more likely to use identity theft protection, credit report security freezes, and credit monitoring than the overall U.S. population.[21]

75. Since elders are more likely to rely on the type of credit monitoring services that Gas South has offered, albeit for only one year, and because a significant number of the victims of the Gas South Data Breach are likely to be over 55 years old, Gas South's offer of a single year of free credit monitoring through Experian Identity Works is woefully inadequate. The Class's Personal Information is likely to be exploited for years, yet Gas South's relief is limited.

Plaintiff's Experience

Plaintiff Lynne Askew

76. Plaintiff Lynne Askew is and at all times mentioned herein was an individual citizen residing in the State of Georgia, in the City of Stockbridge, Henry County.

[20] *Id.* at 9.
[21] *Id.* at 8.

77. Plaintiff Askew is a customer of Gas South, LLC. When she initially signed up for Gas South services, she was required to provide Gas South with her Personal Information, including but not limited to her Social Security number.

78. On or about July 15, 2022, Plaintiff Askew received a mailed Notice of Data Breach Letter, related to NHS's Data Breach that occurred between February 13, 2022 and February 23, 2022. Attached as Exhibit A.

79. The Notice Letter that Plaintiff Askew received informed her that critical PII was accessed by an "unknown actor." The letter stated that the accessible information included her "name, Social Security number" but did not expand on whether additional information was stolen as well. See Exhibit A. Without further information through discovery, Plaintiff Askew cannot be certain of the extent of her breached PII.

80. Plaintiff Askew is alarmed by the amount of her Personal Information that was stolen or accessed, and even more by the fact that her Social Security number was identified as among the breached data on Gas South's computer system.

81. For a couple of months, Plaintiff Askew has been receiving a significantly higher number of spam emails, calls, and texts.

82. Since the Gas South Data Breach, Plaintiff Askew monitors her financial accounts more often. She spends about 15 minutes per week doing so, which is time that she cannot spend on activities she would prefer.

83. Plaintiff Askew formerly purchased a subscription for an identity theft protection service through Lifelock, but since Gas South's Data Breach, she has taken advantage of the one free year of Experian services. She is concerned that after this year, she will be forced to pay for data protection services for life.

84. As a result of the breach, Plaintiff Askew has increased anxiety that she will be subject to identity theft. She now uses 2-step verification on all financial accounts and password protected websites which offer it.

85. Plaintiff Askew is aware that cybercriminals often sell Personal Information and that hers could be abused months or even years after the Gas South Data Breach.

86. Had Plaintiff Askew been aware that Gas South's computer systems were not secure, she would not have entrusted Gas South with her Personal Information, especially including her Social Security number.

87. Due to the Data Breach, Plaintiff Askew anticipates spending time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

Plaintiff's and Class Members' Damages

88. To date, Defendant has done absolutely nothing to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach and data breach.

89. Moreover, Gas South has offered only a paltry one year of identity theft monitoring and identity theft protection through Experian Identity Works. This one-year limitation is inadequate when Gas South's victims are likely to face many years of identity theft.

90. Furthermore, Defendant Gas South's credit monitoring offer and advice to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Gas South expects Plaintiff and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendant merely sent instructions to Plaintiff and Class Members about actions they can affirmatively take to protect themselves.

91. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

92. These services are also inadequate as Gas South fails to acknowledge that many of the victims of its Data Breach are elderly or infirmed and may not be able to adequately protect themselves from fraud and identity theft.

93. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

94. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, credit card fraud, tax return fraud, medical services billed in their names, utility bills opened in their names, and similar identity theft.

95. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Personal Information.

96. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

97. Plaintiff and Class Members also suffered a loss of value of their Personal Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

98. Class Members were also damaged via benefit-of-the-bargain damages. Part of the price these Class Members paid to Defendant was intended to be used by Defendant to fund adequate security of Defendant's computer property and Class Members' Personal Information. Thus, the Class Members did not get what they paid for. Specifically, they overpaid for services that were intended to be accompanied by adequate data security but were not.

99. Plaintiff and Class Members have been damaged by the compromise of their Personal Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

100. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

101. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach.

102. In addition, many Class Members suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

103. Moreover, Plaintiff and Class Members have an interest in ensuring that their Personal Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage

of data or documents containing personal and financial information is not accessible online, is encrypted, and that access to such data is password-protected.

CLASS ACTION ALLEGATIONS

104. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated (the "Class" or "Classes").

105. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> All people who receive services from Gas South and whose Personal Information was compromised as a result of the Data Breach that occurred during the February 2022 Data Breach.

106. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

107. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under O.C.G.A. 9-11-23, *et seq.*

108. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is

unknown to Plaintiff at this time, and according to its Notice letter, its investigation is ongoing, the Class consists of at least 38674 individuals whose data was compromised in the Data Breach.

109. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personal Information;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Personal Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Personal Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

i. Whether Defendant's conduct was negligent, and;

j. Whether Plaintiff and Class Members are entitled to damages and/or injunctive relief.

110. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Personal Information, like that of every other Class Member, was compromised in the Data Breach.

111. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

112. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication

of these common issues in a single action has important and desirable advantages of judicial economy.

113. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

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

115. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Personal Information;

b. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant's failed to take commercially reasonable steps to safeguard consumer Personal Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

116. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

CAUSES OF ACTION

First Count

Negligence
(On Behalf of Plaintiff and All Class Members)

117. Plaintiff realleges and incorporates by reference the allegations in above as if fully set forth herein.

118. Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Personal Information held within it—to prevent disclosure of the information, and to safeguard the information from theft.

119. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a cyberattack.

120. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Personal Information.

121. Defendant's duty of care to use reasonable security measures arose due to the special relationship that existed between it and the Class, which is recognized by laws and regulations including but not limited to common law. Defendant was

in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

122. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

123. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant was bound by industry standards to protect confidential Personal Information.

124. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Personal Information. The specific negligent acts and omissions committed by Defendant includes, but is not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Personal Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failure to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Personal Information;

e. Failing to detect in a timely manner that Class Members' Personal Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

125. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. The breach of security was reasonably foreseeable given the known high frequency of data breaches in recent years.

126. The Data Breach was foreseeable due to Defendant's to adequately safeguard Class Members' Personal Information and was foreseeable that it would result in one or more types of injuries to Class Members.

127. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

128. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate, long-term credit monitoring and identity theft protection to all Class Members.

Second Count
Negligence Per Se
(On Behalf of Plaintiff and All Class Members)

129. Plaintiff realleges and incorporates by reference the allegations above as if fully set forth herein.

130. Pursuant to the FTCA, Gas South was required by law to maintain adequate and reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and Class Members' Personal Information.

131. Gas South breached its duties by failing to employ industry standard data and cybersecurity measures to gain compliance with those laws, including, but not limited to, proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

132. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Personal Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Gas South's networks, databases, and computers that stored or contained Plaintiff's and Class Members' Personal Information.

133. Plaintiff's and Class Members' Personal Information constitutes personal property that was stolen due to Gas South's negligence, resulting in harm, injury and damages to Plaintiff and Class Members.

134. Gas South's conduct in violation of applicable laws directly and proximately caused the unauthorized access and disclosure of Plaintiff's and Class Members' unencrypted Personal Information.

135. Plaintiff and Class Members have suffered and will continue to suffer damages as a result of Gas South's conduct. Plaintiff and Class Members seek damages and other relief as a result of Gas South's negligence.

Third Count
Breach of Implied Contract
(On Behalf of Plaintiff and All Class Members)

136. Plaintiff realleges and incorporates by reference the allegations above as if fully set forth herein.

137. Gas South provides natural gas services to Plaintiff and Class Members. Plaintiff and Class Members also formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services and/or receiving pay for labor or goods from Defendant.

138. Through Defendant's performance of, sale of, and/or purchase of goods and services, it knew or should have known that it must protect Plaintiff's and Class

Members' confidential Personal Information in accordance with Gas South's policies, practices, and applicable law.

139. As consideration, Plaintiff and Class Members paid money to Gas South for natural gas services, or and turned over valuable PII to Defendant. Accordingly, Plaintiff and Class Members bargained with Gas South to securely maintain and store their Personal Information.

140. Gas South violated these contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information and by disclosing it for purposes not required or permitted under the contracts or agreements.

141. Plaintiff and Class Members have been damaged by Gas South's conduct, including by paying for data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

Fourth Count
Invasion of Privacy
(On Behalf of Plaintiff and All Class Members)

142. Plaintiff realleges and incorporates by reference the allegations above as if fully set forth herein.

143. Plaintiff and Class Members maintain a privacy interest in their Personal Information, confidential information that is also protected from

disclosure by applicable laws set forth above. Plaintiff and Class Members' Personal Information was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities.

144. Additionally, Plaintiff's and Class Members' Personal Information, when contained unencrypted and in electronic form, is highly attractive to criminals who can nefariously use their Personal Information for fraud, identity theft, and other crimes without their knowledge and consent.

145. Gas South's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person.

146. Gas South's disclosure of Plaintiff's and Class Members' Personal Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' personal quarters where their Personal Information was stored and disclosed private facts about finances into the public domain.

147. Plaintiff and Class Members have been damaged by Gas South's conduct, including by paying for products and services that should have included

data and cybersecurity protection that they did not receive, as well as by incurring the harms and injuries arising from the Data Breach now and in the future.

Fifth Count
Unjust Enrichment
(On Behalf of Plaintiff and All Class Members)

148. Plaintiff realleges and incorporates by reference the allegations above as if fully set forth herein.

149. Plaintiff and Class Members conferred a benefit on Gas South by paying for products and services that should have included data and cybersecurity protection to protect their Personal Information, which was not provided and Plaintiff and Class did not receive.

150. Gas South has retained the benefits of its unlawful conduct including the amounts received for data and cybersecurity practices that it did not provide. Due to Gas South's conduct alleged herein, it would be unjust and inequitable under the circumstances for Gas South to be permitted to retain the benefit of its wrongful conduct.

151. Plaintiff and the Class Members are entitled to a refund of moneies not spent on data security that should have been as well as restitution and/or damages from Gas South and/or an order of this Court proportionally disgorging all profits, benefits, and other compensation obtained by Gas South from its wrongful conduct.

If necessary, the establishment of a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation may be created.

152. Additionally, Plaintiff and the Class Members may not have an adequate remedy at law against Gas South, and accordingly plead this claim for unjust enrichment in addition to or, in the alternative to, other claims pleaded herein.

Sixth Count
Breach of Confidence
(On Behalf of Plaintiff and All Class Members)

153. Plaintiff realleges and incorporates by reference the allegations above as if fully set forth herein.

154. At all times during Plaintiff's and Class Members' interaction with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Personal Information.

155. As alleged herein and above, Defendant's relationship with Plaintiff's and Class Members was governed by terms and expectations that Plaintiff's and Class Members' Personal Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

156. Plaintiff and Class Members provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit Personal Information to be disseminated to any unauthorized parties.

157. Plaintiff and Class Members also provided their Personal Information to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect such Personal Information from unauthorized disclosure.

158. Defendant voluntarily received in confidence Plaintiff's and Class Members' Personal Information with the understanding that it would not be disclosed or disseminated to the public or any unauthorized third parties.

159. Due to Defendant's failure to prevent, detect, or avoid the Data Breach from occurring by, inter alia, following industry standard information security practices to secure Plaintiff's and Class Members' Personal Information, Plaintiff's and Class Members' Personal Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

160. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and Class Members have suffered damages.

161. But for Defendant's disclosure of Plaintiff's and Class Members' Personal Information in violation of the parties' understanding of confidence, their protected Personal Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' protected Personal Information, as well as the resulting damages.

162. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Personal Information.

163. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Personal Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Personal Information; (iv) lost opportunity costs associated with effort expended to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching to prevent, detect, contest, and recover from financial fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) the continued risk to their Personal Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information of past and current customers in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

164. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

Seventh Count
Violation of the Georgia Uniform Deceptive Trade Practices Act
(Georgia Code Annotated §§ 10-1-370, *et seq*.)
(On behalf of the Class)

165. Plaintiff realleges and incorporates by reference the allegations above as if fully set forth herein.

166. Plaintiff asserts this cause of action on behalf of the Class.

167. As fully alleged above, Defendant engaged in unfair and deceptive acts and practices in violation of Georgia Uniform Deceptive Trade Practices Act (Ga. Code Ann., §§ 10-1-370, *et seq*.).

168. Reasonable individuals would be misled by Defendant's misrepresentations and/or omissions concerning the security of their PII, because they assume companies that collect PII from customers will properly safeguard that Personal Information in a manner consistent with industry standards and practices.

169. Defendant did not inform customers that it failed to properly safeguard their Personal Information, thus misleading Plaintiff and Class members in violation of §10-1-370, *et seq*. Such misrepresentation was material because Plaintiff and Class members entrusted Defendant with their Personal Information.

170. Had Plaintiff and Class members known of Defendant's failure to maintain adequate security measures to protect their Personal Information, Plaintiff and Class members would not have entrusted their Personal Information to Defendant.

171. As a direct and proximate result of Defendant's breach of duty, Plaintiff and Class Members have suffered and will continue to suffer injury and/or harm.

172. Plaintiff seeks restitution and injunctive relief on behalf of the Class, along with attorney's fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage,

and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages and compensatory damages in an amount to be determined, as allowable by law;

g) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h) Pre- and post-judgment interest on any amounts awarded; and

i) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: August 24, 2022

Respectfully submitted,

/s/ *Allison E. McCarthy*
Law Offices of Allie McCarthy
Georgia Bar No. 482220
1055 Prince Avenue, Suite 2
Athens, GA 30606
Phone: (678) 637-6243
attorneymccarthy@gmail.com

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
MASON LLP
5101 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Attorneys for Plaintiff

**pro hac vice to be filed*

EXHIBIT A

GAS SOUTH

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 15, 2022

[redacted]
LYNNE ASKEW
[redacted]
STOCKBRIDGE, GA
[redacted]

Notice of Security Incident

Dear Lynne Askew:

Gas South LLC ("Gas South") writes to notify you about a recent data incident that may involve some of your personal information. This notice provides you with information about the incident, our response, and additional steps you may take to protect your information, should you determine it is appropriate to do so.

What Happened? On February 21, 2022, Gas South discovered suspicious activity on certain Gas South computer systems. Upon identifying unusual activity on certain systems, Gas South disconnected these systems from the network and commenced an investigation. The investigation determined that an unknown actor had access to limited Gas South systems between February 13, 2022 and February 23, 2022. Because the investigation determined that there was unauthorized access to certain data, Gas South initiated a review of its systems to determine the type of information and to whom it related. Following its initial review, Gas South worked diligently to identify and populate address information for any potentially affected individuals. In an abundance of caution, we are notifying you about the event before the investigation is complete so that you may take steps to protect your information.

What Information Was Involved? The impacted Gas South systems stored the following information related to you: name, Social Security number.

What We Are Doing. We take this incident very seriously. Information privacy and security are among our highest priorities, and we have security measures in place to protect information in our care. Upon discovering this incident, we investigated and responded to the incident, and are reviewing and enhancing our existing policies and procedures to reduce the likelihood of a similar future event. Gas South reported this incident to federal law enforcement and is notifying potentially affected individuals and relevant regulators as required.

Moreover, as an added precaution, Gas South is offering complimentary access to credit monitoring and identity restoration services to you for 12 months through Experian because your information may have been present in the systems accessed during the incident.

What You Can Do. Gas South encourages you to remain vigilant against incidents of identity theft and fraud. Be wary of unknown callers, emails or text messages, regularly review your bank and pension accounts for unusual activity and explanation of benefits and review your free credit reports for suspicious activity. You may also review and consider the information and resources outlined in the below "Steps You Can Take to Help Protect Personal Information."

0022850

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12 months membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by October 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code:** [redacted]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 420-2830** by **October 31, 2022**. Be prepared to provide engagement number **B055471** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For More Information. If you have additional questions, please call our dedicated assistance line at (833) 420-2830 toll-free Monday through Friday from 9 am – 11 pm ET, or Saturday and Sunday from 11 am – 8 pm ET (excluding major U.S. holidays). Be prepared to provide your engagement number B055471. You may write to Gas South at One Overton Park, Atlanta, GA, 30339 with any additional questions you may have.

Sincerely,

Gas South LLC

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

ClassAction.org