THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

EZ MART 1, LLC, on behalf of itself and all others similarly situated, **Plaintiff,** **v.** **COLONIAL PIPELINE COMPANY,** **Defendant.**	**COMPLAINT-CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiff EZ Mart 1, LLC, individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Defendant Colonial Pipeline Company and alleges, upon personal knowledge as to its own actions and its counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION.

1. Plaintiff brings this class action against Defendant for its failure to properly secure "the largest pipeline system for refined oil products in the U.S…. consisting of two tubes … 5,500 miles (8,850 km) long … and [capable of carrying] 3 million barrels [more than 100 million gallons] of fuel per day between Texas and

New York" (the "Pipeline").[1]

2. On May 7, 2021, Defendant learned that cybercriminals had performed a ransomware attack against Defendant's systems, which encrypted or "locked" certain data thereon (the "Ransomware Attack").

3. By the end of the day, Defendant paid the cybercriminals a $4.4 million ransom in return for a decryption tool that would allow Defendant to retrieve the encrypted or "locked" data.

4. Even with the decryption tool, it took approximately five (5) days for Defendant to restart the Pipeline.

5. The five-day shutdown of the Pipeline resulted in fuel shortages in areas that the Pipeline serviced, affecting more than 11,000 gas stations and causing a sharp increase in the price of gasoline for automobiles and other motor vehicles and a sharp decrease in convenience store sales.

6. Plaintiff brings this action on behalf of the more than 11,000 gas stations negatively impacted by the Ransomware Attack.

7. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. This injury includes: (1) a fuel shortage that limited or prevented Plaintiff and Class Members from selling fuel – and, as a result, other

[1] https://en.wikipedia.org/wiki/Colonial_Pipeline (last visited June 17, 2021).

products – to their customers and (2) an increase in the price of gasoline, which reduced the profitability of Plaintiff's and Class Members' operations.

8. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the Pipeline's critical infrastructure was safeguarded. As a result, Plaintiff and Class Members were subjected to a sudden and dramatic fuel shortage and increase in the price of gasoline and suffered damages. In addition, Plaintiff and Class Members have a continuing interest in ensuring that Defendant safeguards the Pipeline's critical infrastructure, and they are therefore entitled to injunctive and other equitable relief.

II. PARTIES.

9. Plaintiff EZ Mart 1, LLC is a limited liability company organized under the laws of North Carolina and located at 1619 Castle Hayne Road in Wilmington, New Hanover County, North Carolina. It is owned by Abeer Darwich, the president of the LLC, and operated by her husband, Ahmad "Eddie" Darwich.

10. The Darwiches have operated the EZ Mart on Castle Hayne Road for approximately 11 years. The business consists of two gas pumps, featuring unleaded and premium gasoline, as well as a separate pump for diesel fuel. In addition to selling gas, the EZ Mart is a convenience store that sells food, tobacco products, beer

and soft drinks, among other things.

11. Plaintiff EZ Mart 1, LLC purchases its fuel from a fuel and oil distributor, Oliver's Oil Company, in Lumberton, North Carolina, which upon information and belief purchases all or some of its petroleum products directly or via one or more intermediaries from Defendant Colonial Pipeline Company.

12. Defendant Colonial Pipeline Company is a corporation organized under the laws of Delaware; it is also incorporated in Virginia. Defendant has a principal place of business and corporate headquarters in Alpharetta, Georgia, and it may be served with process at its office at 1185 Sanctuary Parkway, Suite 100, Alpharetta, Georgia 30009, or through its registered agent, CSC of Cobb County, Inc., 192 Anderson Street SE, Suite 125, Marietta, Georgia 30060.

13. Defendant's corporate executives and decisionmakers work out of its Alpharetta headquarters. Defendant's policies and procedures are originated out of that corporate office and its computer systems and infrastructure are centralized in or controlled out of that office. Defendant's "control center" where the electronic ransom note was discovered is at its headquarters.

14. The true names and capacities of other persons or entities, whether individual, corporate, associate, or otherwise, who may be additionally responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff

will seek leave of Court to amend this complaint to reflect the true names and capacities of such other responsible parties when and if their identities become known and it appears otherwise appropriate to do so.

15. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE.

16. This Court has subject matter and diversity jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

17. This Court has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Georgia including via the operation of its headquarters.

18. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) & (2) because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

IV. FACTUAL ALLEGATIONS.

A. Background.

19. Defendant operates the Pipeline, the largest such system in the United States for refined oil products. Defendant has a virtual monopoly in its role in gasoline supply for multiple parts of the East Coast.

20. Plaintiff and Class Members relied on Defendant to keep the Pipeline operating so that Plaintiff and Class Members could sell fuel to their customers.

21. Defendant had a duty to adopt reasonable measures to ensure the continued and uninterrupted operation of the Pipeline.

22. Defendant's Pipeline is essential infrastructure and a vital artery for the distribution and delivery of fuel to most of the eastern United States, in particular for the gas station and convenience store owners who depend upon its lifeline.

23. As discussed below, the nature of Defendant's security lapse for its electronic systems was basic and grossly negligent. It occurred despite advance knowledge and warnings, including prior cybersecurity incidents involving pipelines. In the lead-up to the electronic break-in, Defendant had repeatedly ignored and rejected efforts by the applicable regulatory agency to meet with it so as to check on its cybersecurity. Defendant is a lucrative and well-resourced company which paid $670 million in dividends to its owners in 2018 and the

incremental cost to the company to take the basic steps it did not take to secure its systems was minimal. It had no plan in place for ransomware attacks and had left up a legacy VPN system without shutting off logins and passwords for old employees – a basic failure according to Defendant's own later-retained experts.

24. The nature of the data stolen or exfiltrated by the threat actors who engaged in the ransomware attack on information and belief included customer and billing information and the present whereabouts of that data are unknown. On information and belief, Defendant elected to shut down the pipeline in whole or part not because the threat actor had reached the operational systems, but because Defendant was not sure it could continue to accurately bill for the product moving through its Pipeline.

25. The sudden shutdown of the Pipeline on May 7, 2021 was a sudden and calamitous event that jeopardized the business of the Plaintiff. Defendant had touted in public relations materials that it placed its obligations to its customers and the public first but this was not the case in this instance. In Congressional hearings after the incident, Defendant has acknowledged its duty to those affected by the failure, but to date has failed to offer them any compensation or remedy. Defendant has stated the ransom it decided to pay despite FBI guidance not to do so, is covered by its cybersecurity insurance. The nature of the harm to the Plaintiff was foreseeable.

26. Under all the facts and circumstances, Defendant owed a duty running to Plaintiff and other similarly situated gas station and convenience store owners to take basic steps to secure its electronic systems and protect against cyber-intrusions and data breaches so as to ensure the uninterrupted delivery and distribution of fuel to Plaintiff and Class Members.

B. The Ransomware Attack.

27. On May 7, 2021, Defendant learned that cybercriminals had performed the Ransomware Attack, thereby breaching and exfiltrating or stealing voluminous data of the company and encrypting data on Defendant's systems. In fact, as was subsequently learned, the threat actor who engaged in the attack had been on Defendant's computer system for a full week without detection, free to roam and copy materials. Defendant did not have a cybersecurity program encompassing ransomware issues in place at the time of this attack and data breach. As a result of the Ransomware Attack, Defendant elected to completely suspend operation of the Pipeline.

28. Many of the details of the root cause of the attack, the vulnerabilities exploited, and the remedial measures undertaken to ensure a similar attack does not occur again have not been shared with the general public, Plaintiff or Class Members, who retain a vested interest in the Pipeline's uninterrupted operation.

29. However, analysis to date of the cyberattack on Colonial Pipeline has determined that hackers were able to access the company's network by using a compromised virtual private network ("VPN") password.

30. A VPN extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

31. Many companies prefer to use a VPN in addition to the private network found at their corporate offices. This is because by using the VPN, company employees can log in remotely from a physical location that is not at the company offices.

32. However, the use of a VPN brings with it obvious cybersecurity threats, because the individuals logging into the company's computer system are not restricted to simply those who are physically on site at the company offices.

33. To prevent disclosure of private information, VPNs typically allow only authenticated remote access using "tunneling" protocols and encryption techniques. Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor or multi-factor authentication or other cryptographic methods.

34. For networks with national security implications, and which provide essential infrastructure, such as the Defendant's Pipeline as Defendant itself admits in public pronouncements, it is grossly negligent to require nothing more by way of authentication than a simple login and password, including that of an old worker on an outdated and superseded system, to access to inner workings of the company's system and to allow a data breach including on information and belief unfettered access by the hackers to the sensitive and private data of Pipeline distributors, customers and users.

35. At some point in the past, Defendant switched from its old remote access system to one using two-factor or multi-factor authentication. However, when Defendant did so, it inexplicably left its old, less secure system intact and operational. Defendant took no steps to disable or eliminate the old system nor to eliminate the ability of departed employees – or bad actors who have stolen employee credentials – to access it undetected.

36. The Ransomware Attack actors gained access to the company's computer networks by using a compromised employee password.

37. The password had been linked to Defendant's disused VPN account for remote access. This account was not guarded by an extra layer of security via multi-

factor authentication. There was no mechanism, for example, for use of a one-time password to ensure security.[2]

38. States differently, the password was associated with an outdated "legacy" VPN platform. The platform had been replaced by the company's newer system using multi-factor authentication using RSA tokens.[3] For whatever reason, when Defendant put up its new platform, it neglected to take down its old one.

39. The hackers had apparently found the password from data on the dark web. The login and password were outdated in that they were no longer used by any employees, but they were still valid in the Colonial Pipeline network and allowed the attackers to enter the network on April 29, 2021. The employee who had used the login and password on Colonial's old system had apparently also used it on another website that got hacked.

[2] Prepared Statement of Charles Carmakal, Senior Vice President and Chief Technology Officer, FireEye-Mandiant, before the United States House Committee on Homeland Security, June 9, 2021 ("The earliest evidence of compromise that we have identified to date occurred on April 29, 2021. On that date, the threat actor had logged into a virtual private network (VPN) appliance using a legacy VPN profile and an employee's username and password. The legacy VPN profile did not require a one-time passcode to be provided. The legacy VPN profile has since been disabled as part of Colonial Pipeline's remediation process.").

[3] RSA tokens are part of a remote-access security system offered by RSA Security.

40. After entering the system, the attackers explored the Colonial Pipeline computer system for approximately a week, wholly undetected, before sending the ransom note and activating the ransomware.

41. Colonial's computer system includes voluminous information related to the intricate web of gas and oil product suppliers and customers. This information is used by Colonial for billing purposes and the company possesses voluminous private and sensitive information regarding suppliers and customers. When the suppliers and customers provide sensitive and private billing, accounting and financial information to Colonial, they do so under an expectation that the company will keep the information private and take reasonable steps to safeguard the information.

42. When the breach first occurred on April 29, 2021, it was not discovered. After the hackers had reviewed and stolen or exfiltrated data for a week, they then used software to encrypt or disable some of the billing and other systems on Defendant's computer system. This encryption however did not extend to include Defendant's separately siloed Pipeline control systems. However, Defendant lacked either the trained management or the action plan to promptly assess the ransomware once installed. The threat actor put up the electronic ransomware note on the Colonial computer system which was discovered at or about 5 a.m. on May 7, 2021

by a control room employee in the Alpharetta, Georgia headquarters control room who saw the ransomware note on the system. He brought the matter to his supervisor in the control room. According to Defendant, it decided to shut down the Pipeline at about 6 a.m.

43. As noted, the login and password that the attackers used were for the remote access account of an inactive employee. Even though the employee had left Colonial Pipeline, Defendant allowed the account to remain active. When an employee leaves a company, the proper practice is to shut down their login and password. However, Defendant neither did that, nor had in place an effective audit system to check and make sure accounts of departed employees could not be used, nor did Defendant take steps to ensure the old remote access system was shut down once a new system was acquired.

44. FBI and government guidance states that those receiving ransom demands from ransomware attackers should not pay the ransom. However, by the end of May 7 Defendant elected to negotiate with the hackers and pay the ransom on May 8. Defendant has since stated that it has cybersecurity insurance that it expects will cover the entire amount of any ransom loss of Defendant.

45. Reports have varied as to why Defendant felt it necessary to immediately shut down the Pipeline system. On information and belief, the

company halted operations because its billing system was compromised, and Defendant was concerned that it would be able to determine how much to bill customers for fuel they received.[4]

C. Additional facts on Defendant's failure to use proper procedures.

46. Defendant did not use reasonable security procedures and practices appropriate to operating the largest Pipeline system in the United States for refined petroleum products in the time period leading up to the attack.

47. As explained by the FBI, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[5]

48. To prevent and detect ransomware attacks, including the one that occurred here, Defendant could and should have implemented the following measures:

---

[4] Natasha Bertrand, Evan Perez, Zachary Cohen, Geneva Sands and Josh Campbell, Colonial Pipeline did pay ransom to hackers, sources now say, CNN, May 13, 2021 ("The company halted operations because its billing system was compromised, three people briefed on the matter told CNN, and they were concerned they wouldn't be able to figure out how much to bill customers for fuel they received. One person familiar with the response said the billing system is central to the unfettered operation of the pipeline. That is part of the reason getting it back up and running has taken time, this person said."). At https://www.cnn.com/2021/05/12/politics/colonial-pipeline-ransomware-payment/index.html (last visited June 18, 2021).

[5] *See* Ransomware Prevention and Response for Chief Information Security Officers, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited June 17, 2021).

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Educate top management on ransomware and similar cybersecurity threats, and designate an executive management position to handle cybersecurity issues.

- Ensure that old VPN remote access systems are taken down when new ones are instituted.

- Ensure that employee logins and passwords that are no longer being used are turned off and disabled.

- Allow government agencies charged with the mission of assisting private industry to ensure their adequate cybersecurity are given recognition and cooperation, rather than rejecting their efforts to assist.

- Ensure that when it comes to a private company that holds an effective monopoly and a bottleneck over critical infrastructure with national security implications, that company does not use VPN remote access with lax security measures.

- Require two-factor or multi-factor authentication for any and all remote access to the company's computer systems.

- Require a policy that in the event that it becomes necessary to continue the flow of the product, with the possibility that Colonial may not be able to bill for it, versus turning off that flow abruptly to the jeopardy of customers and the nation, the former choice is made.

- Ensure regular, thorough cybersecurity audits.

- Engage outside cybersecurity consultants and firms to ensure industry standards are met for cybersecurity for the company.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and

Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/ LocalAppData folder.
- Disable Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a

virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[6]

49. To prevent and detect ransomware attacks, including the instant attack, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures, in addition to those alleged elsewhere herein:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is

[6] *Id.* at 3-4.

> legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA [the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency] product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[7]

50. To prevent and detect ransomware attacks, including the Ransomware Attack, Defendant could have, and should have, implemented the following measures recommended by the Microsoft Threat Protection Intelligence Team, in addition to the measures alleged elsewhere herein:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential

[7] *See* Cybersecurity & Infrastructure Security Agency, Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited June 17, 2021).

full compromise;

Include IT Pros in security discussions

- Ensure collaboration among security operations, security admins, and information technology admins to configure servers and other endpoints securely;

Build credential hygiene

- Use multifactor authentication or network level authentication and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and Antimalware Scan Interface for Office [Visual Basic for Applications].[8]

51. Given that Defendant was operating the largest Pipeline system in the United States for refined petroleum products, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

[8] Adapted from Microsoft 365 Defender Threat Intelligence Team, Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited June 17, 2021).

52. The occurrence of the Ransomware Attack indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Ransomware Attack and a fuel shortage that impacted more than 11,000 gas stations, including Plaintiff and Class Members.

53. Defendant's failure to detect and prevent the Ransomware Attack was compounded by its unreasonable refusal, both before and after the Ransomware Attack, to participate in security assessments.

54. It was reported on June 15, 2021, that the Transportation Security Administration ("TSA") "prior to the attack asked Colonial Pipeline on no less than thirteen occasions to participate in physical and cyber pipeline security assessments. Citing COVID-19, Colonial repeatedly delayed and chose not to participate. On multiple occasions, Colonial didn't even bother responding to TSA's emails. In fact, Colonial still has not agreed to participate in the physical assessment, and only agreed to cooperate with TSA's cybersecurity assessment three weeks after the ransomware attack occurred."[9]

55. Colonial's unreasonable refusal to participate in cyber pipeline security

[9] Committee on Homeland Security, Joint Hearing Statement of Transportation & Maritime Security Subcommittee Chairwoman Bonnie Watson Coleman (D-NJ), *Cyber Threats in the Pipeline: Lessons from the Federal Response to the Colonial Pipeline Ransomware Attack*, at 1 (June 15, 2021).

assessments reflected deliberate indifference to its obvious and well-established duty to Plaintiff and Class Members: "when you operate infrastructure that we all depend on, you have a responsibility to the public."[10]

56. Defendant's shutdown of the pipeline was a sudden calamitous event that jeopardized the security and livelihoods of those who depend upon ready access to gasoline for a variety of uses and reasons.

57. Defendant halted the pipeline on May 7, 2021. The pipeline remained shut down on May 8, May 9, May 10 and May 11. The restart of pipeline operations did not begin until 5 p.m. on May 12, ending a six-day shutdown. However, even then, it took some time thereafter for service to return to normal.

58. As of May 12, 2021, it was estimated that gas stations in affected states were out of gas as follows: NC: 65%; VA: 44%; GA: 43%; SC: 43%; TN: 16%; FL: 11%; MD: 11%; DC: 10%; W. VA: 4%; AL: 7%; MS: 5%; KY: 2%.[11]

D. Facts regarding the Plaintiff.

59. On or around May 10, 2021, Plaintiff EZ Mart's owner Abeer Darwich and her husband Ahmad "Eddie" Darwich, began hearing that some sort of

[10] *Id.* at 2.

[11] Colonial Pipeline begins pumping gas again after Russian cyberattack shut it down for six days, May 12, 2021, at https://newsbinding.com/uk-news/colonial-pipeline-begins-pumping-gas-again-after-russian-cyberattack-shut-it-down-for-six-days/ (last visited June 20, 2021).

cyberattack had shut down the Colonial Pipeline and petroleum supplies in the Southeast would be impacted.

60. On May 11, 2021, even as consumers began scrambling for available fuel, EZ Mart's daily sales inside its convenience store began to nosedive.

61. On May 12, 2021, EZ Mart sold the last of its fuel, placing baggies on the handles of its pumps to let fuel-seeking customers know they were out. The EZ Mart's pumps require payment inside the store rather than at the pumps.

62. On or around May 12, 2021, Mr. Darwich called his longtime distributor, Oliver's Oil, and asked when he might get more fuel delivered. He was told that it depended on when the pipeline was flowing again and the distribution chain returned to normal.

63. It was not until May 21, 2021, that EZ Mart's pumps were at full capacity again.

64. In the meantime, in addition to the loss of gasoline sales, Plaintiff EZ Mart saw inside sales drop precipitously. Due to the Pipeline Ransomware attack and attendant fuel shortage, Plaintiff EZ Mart's sales for May ($76,185) fell by $7,789 compared to sales for April ($83,974), even though the EZ Mart is located on a busy thoroughfare outside a popular coastal city and May is the beginning of tourist season.

E. Defendant knew or should have known of the dangers.

65. In the years and months leading up to May 7, 2021, the dangers of ransomware attacks had become well-known among IT professionals and computer systems managers at large corporations such as Defendant. Defendant was well-aware of the quantity of critical and commercially sensitive information in its computer systems. And Defendant is a massively resourced company owned by some of the largest gas and oil interests in the world. However, Defendant had failed to take reasonable steps to secure and protect its systems against data breach and ransomware attacks.

66. Ransomware attacks have been known to occur for years. Furthermore, in the months leading up to May 7, 2021, the number and scope of ransomware attacks had expanded, and this fact was known to those in the IT industry.

67. Defendant's own retained consultant, Mandiant, described after the instant attack that "[i]n 2015, Mandiant observed a notable surge in disruptive intrusions in which threat actors deliberately destroyed critical business systems, leaked confidential data, taunted executives, and extorted organizations."[12]

[12] Prepared Statement of Charles Carmakal, Senior Vice President and Chief Technology Officer, FireEye-Mandiant, before the United States House Committee on Homeland Security, June 9, 2021.

68. "The problem has steadily grown worse in recent years, and in 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware, according to the security firm Emsisoft."[13]

69. In addition, for years, it had been known and publicized that critical infrastructure such as pipelines were especially vulnerable to the assaults of both conventional and cyber-criminals, and that therefore investing adequately in cyber-security was essential for those who desired to be in the pipeline business.

70. Pipelines in the United States have been the target of several confirmed terrorist plots and attempted physical attacks since September 11, 2001.[14]

71. In 2011, the computer security company McAfee reported "coordinated covert and targeted" cyberattacks originating primarily in China against global energy companies. The attacks began in 2009 and involved a hacking tactic known as "spear-phishing," exploitation of Microsoft software vulnerabilities, and the use

[13] Ransomware Task Force, Institute for Security and Technology, Combating Ransomware, A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force, p. 7, https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf (last visited June 21, 2021).

[14] Paul W. Parfomak, Pipeline Cybersecurity: Federal Policy, August 16, 2012, Congressional Research Service.

of remote administration tools to collect sensitive competitive information about oil and gas fields.[15]

72. In 2012, authorities warned that changes to pipeline computer networks over the years, the emergence of more sophisticated hackers, and the development of specialized malicious software had made pipeline supervisory control and data acquisition operations increasingly vulnerable to cyberattacks.[16]

73. In 2011-12, there were a coordinated series of cyber intrusions specifically targeting U.S. pipeline computer systems.[17] From December 2011 through June 2012, cyberspies linked to China's military targeted nearly two dozen U.S. natural gas pipeline operators. The attack targeted 23 gas pipeline companies, according to information from the Department of Homeland Security ("DHS") and the DHS's Industrial Control Systems Cyber Emergency Response Team ("ICS-CERT").[18]

---

[15] Prepared Statement of Paul W. Parfomak, April 19, 2016, to the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, April 19, 2016.
[16] *Id.*
[17] *Id.*
[18] Mark Clayton, Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage, Christian Science Monitor, February 27, 2013; Kevin E. Hemsley and Dr. Ronald E. Fisher, History of Industrial Control System Cyber Incidents, Dec. 2018, INL/CON-18-44411-Revision-2, p. 10; Gas Pipeline Cyber Intrusion Campaign – Update, ICS/CERT Monthly Monitor, June-July 2012.

74. After the 2011-12 attacks occurred, ICS-CERT broadly disseminated information about the attacks to asset owners and operators.[19] On information and belief this included dissemination to representatives of Defendant.

75. In 2013, ICS-CERT, in coordination with the FBI, the U.S. Department of Energy ("DOE"), the Electricity Sector Information Sharing and Analysis Center ("ES-ISAC"), the TSA, and the Oil and Natural Gas and Pipelines Sector Coordinating Councils Cybersecurity Working Group, conducted a series of 14 action campaign briefings in response to the growing number of cyber-incidents related to U.S. critical infrastructure. The briefings were given to over 750 attendees in cities throughout the country to assist critical infrastructure asset owners and operators in detecting intrusions and developing mitigation strategies.[20] On information and belief, Defendant's representatives attended these briefings.

76. In 2013, congressional hearings were held on the subject of critical infrastructure and cyber threats. Those who testified at these hearings noted, among other things, that "pipeline networks … are susceptible … to internet-delivered attacks."[21]

---

[19] *Id.*
[20] *Id.*
[21] Statement of Dean Picciotti, Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure, hearing before the Subcommittee on

77. In a campaign lasting from early 2013 through 2014, an allegedly Russia-backed group known as Dragonfly or Energetic Bear targeted electricity distribution, electricity generation, oil pipeline and energy industry industrial equipment manufacturers via supply chain cyberattacks.[22]

78. In 2016, during further congressional hearings, speakers noted the need to "thwart malicious actors with ill intentions from damaging or disrupting pipeline operations" and that "[i]n addition to physical attacks, we must also guard against cyber attacks." The speakers noted that "adversaries … have shown a proclivity for launching sophisticated cyber attacks against U.S. companies, banks, and critical infrastructure." There had been "several high-profile incidents where the systems of global energy companies have been compromised and sensitive information fell into the wrong hands."[23] Speakers discussed "pipeline data security," and techniques

---

Cybersecurity, Infrastructure Protection, and Security Technologies, of the Committee on Homeland Security, House of Representatives, 113th Congress, First Session, March 20, 2013.

[22] Booz Allen, Industrial Cybersecurity Threat Briefing, 2016, p. 15; Kevin E. Hemsley and Dr. Ronald E. Fisher, History of Industrial Control System Cyber Incidents, Dec. 2018, INL/CON-18-44411-Revision-2, p. 3.

[23] Statement of Hon. John Katko, Chairman, U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, hearing entitled Pipelines: securing the veins of the American economy, April 19, 2016.

for "pipeline operators defend their systems from cyber attacks,"[24] and noted that "cybersecurity threats to pipelines have been increasing."[25] The President of the Association of Oil Pipe Lines promised that the pipeline industry was focused on "being prepared for cyber attacks."[26]

79. In a 2017 report, the Congressional Research Service described that "[w]hile physical threats to the U.S. power grid and pipelines have long worried policymakers, cyber threats to the computer systems that operate this critical infrastructure are an increasing concern."[27] The report found that the "secure operation of both the power grid and pipelines are national priorities and that "the electricity grid and energy pipelines are under the same types of cybersecurity risks as other industries, such as financial services or transportation."[28]

80. In January 2019, the Director of National Intelligence in a statement for the record described that "China has the ability to launch cyber attacks that cause

[24] Statement of Andrew J. Black, President and CEO, Association of Oil Pipe Lines, to the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, April 19, 2016.
[25] Prepared Statement of Paul W. Parfomak, April 19, 2016, to the U.S. House of Representatives, Committee on Homeland Security, Subcommittee on Transportation Security, April 19, 2016.
[26] Congressional Research Service, Cybersecurity for Energy Delivery Systems: DOE Programs, August 28, 2017, executive summary.
[27] *Id.*
[28] *Id.*, pp. 1-2.

localized, temporary disruptive effects on critical infrastructure—such as disruption of a natural gas pipeline for days to weeks—in the United States."[29]

81. An August 2019 Government Accountability Office ("GAO") report described that "nation-state, state-sponsored, and state-sanctioned groups or programs, use cyber tools as part of their information-gathering and espionage activities." The report noted that "China and Russia pose the greatest cyberattack threats" with "the ability to disrupt a natural gas pipeline for days to weeks."[30]

82. In February 2020, a ransomware attack on a natural-gas pipeline operator halted operations for two days.[31] The alert from the Cybersecurity and Infrastructure Security Agency ("CISA") described a ransomware attack on an unnamed natural-gas pipeline operator that halted operations for two days while staff shut down, then restored, systems. The alert said that although staff did not lose control of operations, the company did not have a plan in place for responding to a cyberattack.

---

[29] Daniel R. Coats, Director of National Intelligence, Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, p. 5, Jan. 29, 2019, Senate Select Committee on Intelligence https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[30] GAO, Report to Congressional Requesters, Critical Infrastructure Protection: Actions Needed to Address Significant Cybersecurity Risks Facing the Electric Grid, August 2019, GAO-19-332, p. 17 https://www.gao.gov/assets/gao-19-332.pdf

[31] Ransomware Task Force, Combating Ransomware, *supra*, p. 8.

83. In the weeks and months leading up to the Ransomware Attack on May 7, 2021, Defendant rejected offers by government agencies to assess its cyber security defenses. In hearings occurring after the attack, speakers were "troubled by reports that Colonial declined repeated offers by TSA over the past year to assess its security defenses."[32]

84. TSA's Critical Facility Security Review ("CFSR") examines and provides security recommendations on pipeline facilities, while the Validated Architecture Design Review ("VADR") assesses cybersecurity and has been available in virtual format at least since July 2020. However, in hearings occurring after the Ransomware Attack, Defendant's CEO Joseph Blount admitted that Defendant had failed to agree to work and meet with the TSA in that regard in the months leading up to the attack.[33]

85. Those hearings also revealed that as noted above, in the weeks and months leading up to the Ransomware Attack, Defendant had an old log in system it forgot to shut down. This old system allowed remote access without the safety of

[32] Hearing Statement of Chairman Bennie G. Thompson (D-MS), for hearing on Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure, June 9, 2021.

[33] Jule Pattison-Gordon, US House Interrogates Colonial Pipeline CEO Joseph Blount, June 10, 2021, Government Technology, https://www.govtech.com/security/us-house-interrogates-colonial-pipeline-ceo-joseph-blount?_amp=true (accessed June 18, 2021).

double authentication measures that have been offered by software companies for years. Despite its special duty to use safety measures due to its role in national security and essential infrastructure, Defendant had failed to ensure that those seeking remote access could not log in except by multi-factor authentication so as to make sure the person using the computer was who he or she claimed to be. Because Colonial had left up a system that did not use multi-factor authentication, this allowed the hackers to access its network with a compromised username and password.

86. During the pertinent times, Defendant engaged in rudimentary cyber security failures and did not even have a Chief Information Security Officer.[34] The manner in which the breach occurred, by use of stolen credentials, was consistent with the number one vector for data breaches in 2019.[35]

87. Under the facts and circumstances, Defendant was aware of a substantial cyber security risk dating back for years but failed to implement

[34] Colonial Pipeline hackers gained access via unprotected VPN account: password leaked, no MFA, The Stack (describing "rudimentary cyber hygiene failures at the pipeline company, which did not have a Chief Information Security Officer"), https://thestack.technology/how-the-colonial-pipeline-hack-happened/ (accessed June 18, 2021).

[35] *Id.* ("Stolen credentials were the number one vector for data breaches in 2019, according to this Verizon Data Breach report.").

reasonable security measures to combat it.[36] Defendant held a duty toward the gas station and convenience store customers who were dependent upon Defendant maintaining cybersecurity, thereby barring application of the economic loss rule.

88. Oil and gas products are a critical national resource and Defendant holds an effective monopoly and a bottleneck over that resource. Under the circumstances, Colonial had a duty to maintain the supply of fuel to gas stations, whether it wanted to or not, and suspended pipeline operations to the detriment of Plaintiff and those similarly situated at its peril.

89. By engaging in the business of supplying fuel to more than 11,000 gas stations and adopting a critical role in national security and essential infrastructure, and reaping the monetary benefits thereof, Defendant voluntarily assumed a special and independent duty to take reasonable measures to ensure the continued and uninterrupted supply of fuel to the gas stations that relied on such supply.

V. CLASS ACTION ALLEGATIONS.

90. Plaintiff brings this nationwide class action on behalf of itself and on

[36] Lawmakers Chide Colonial Pipeline for Weak Cybersecurity, June 9, 2021, Bloomberg News ("'If your pipeline provides fuel to 45% of the East Coast, why are you only hardening systems after an attack? Why wasn't it done beforehand?' said Rep. John Katko (R-N.Y.), ranking member of the House Homeland Security Committee, which held a hearing June 9 on lessons learned from the attack."). At https://www.ttnews.com/articles/lawmakers-chide-colonial-pipeline-weak-cybersecurity (accessed June 18, 2021).

behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

91. The class that Plaintiff seeks to represent is defined as follows:

> All gas stations that experienced a fuel shortage, an increase in the price paid for gasoline, or an inability to sell fuel to their customers as a result of the Ransomware Attack (the "Nationwide Class").

92. Excluded from the Nationwide Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

93. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

94. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class is so

numerous that joinder of all members is impracticable. More than 11,000[37] gas stations experienced a fuel shortage, an increase in the price paid for gasoline, and/or and an inability to sell fuel to their customers due to the Ransomware Attack.

95. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to safeguard the Pipeline's critical infrastructure running to the Plaintiff and the Class;

b. Whether Defendant failed to adequately safeguard the Pipeline's critical infrastructure during the pertinent times;

c. When Defendant actually learned of the Ransomware Attack;

d. Whether the Ransomware Attack led to the theft or exfiltration of billing and customer data and what is the current status of that data;

e. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to operating the Pipeline;

[37] *See, e.g.,* Daniel Villarreal, Colonial Pipeline Has New Outage with 11,000 Gas Stations Shut, Prices at 7-Year Highs, Newsweek, May 18, 2021 (noting that "over 11,000 gas stations across the nation remain closed due to fuel shortages"), available at https://www.newsweek.com/colonial-pipeline-has-new-outage-11000-gas-stations-shut-prices-7-year-highs-1592715 (last visited June 19, 2021); Irina Slav, Prices At The Pump Stuck At 7-Year Highs, Oilprice.com, May 18, 2021 ("Reuters reports prices were at the highest in seven years, and almost 11,670 gas stations remained closed on Monday, according to data from GasBuddy. The latest data from the company shows a decline in that number, to 11,217 stations."), available at https://oilprice.com/Energy/Energy-General/Prices-At-The-Pump-Stuck-At-7-Year-Highs.html (last visited June 19, 2021).

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Ransomware Attack to occur;

g. Whether Plaintiff and Class Members are entitled to actual, consequential or nominal damages as a result of Defendant's wrongful conduct; and

h. Whether Plaintiff and Class Members are entitled to equitable or injunctive remedies or restitution as a result of Defendant's wrongful conduct.

96. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all experienced a fuel shortage, an increase in the price paid for gasoline, and/or an inability to sell fuel, and therefore other products, to their customers as a result of the Ransomware Attack, which in turn was due to Defendant's misfeasance.

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

98. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that it has no disabling conflicts of interest that would be antagonistic to those of the other members of the Nationwide Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Nationwide Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

99. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose

a burden on the courts.

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

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

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

103. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly safeguard the Pipeline's critical infrastructure and Defendant may continue to act unlawfully as set forth in this Complaint.

104. Further, Defendant has acted or refused to act on grounds generally applicable to the Nationwide Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

VI. CHOICE OF LAW.

105. Defendant's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Georgia and its actions and inactions complained of occurred in, and radiated from, Georgia.

106. The key wrongdoing at issue, constituting Defendant's failure to employ reasonable computer and data security measures emanated from its headquarters in Georgia.

107. Defendant's central control room for its pipeline system is located in its corporate headquarters in Georgia.

108. The ransom note was detected by a control room worker in the early morning of May 7, 2021 at the headquarters in Georgia.

109. The decision to suspend pipeline operations was made by the central management team located in the corporate headquarters in Georgia.

110. The sudden calamitous event of the shutdown of the Pipeline occurred based on control measures undertaken at the headquarters in Georgia.

111. Defendant's key control room, computer and IT personnel operate out of and are located at its headquarters in Georgia. For example, Defendant has recently promulgated help-wanted postings for managerial positions including with computer-related duties at its Alpharetta headquarters.

112. Defendant's policies and procedures pertaining to cybersecurity, such as they were, were set by corporate management in Alpharetta, Georgia.

113. Georgia, which seeks to protect the rights and interests of Georgia and other U.S. businesses against a company doing business in Georgia, has a greater interest in the claims of Plaintiff and the Class members than any other state and is intimately concerned with the outcome of this litigation.

114. Application of Georgia law to a Nationwide Class with respect to Plaintiff's and the class members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of the Plaintiff and the class.

115. Defendant's generic agreements with contractors and vendors have a governing law provision that directs that Georgia law should apply to disputes.[38]

116. Under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia applies to the claims of all class members.

VII. CLAIMS FOR RELIEF

COUNT I – NEGLIGENCE AND GROSS NEGLIGENCE (On Behalf of Plaintiff and the Nationwide Class)

117. Plaintiff repeats and fully incorporates all factual allegations contained in the foregoing paragraphs 1 through ~~112~~ 116 as if fully set forth herein.

118. Defendant owed a duty to Plaintiff and the Nationwide Class to exercise reasonable care to safeguard the Pipeline's critical infrastructure, including protecting it from ransomware attacks, and to safeguard the flow of the product, as a critical resource over which Defendant exercised control.

119. Defendant breached its duties by failing to exercise reasonable care to safeguard the Pipeline's infrastructure, resulting in the Ransomware Attack and Plaintiff and the Nationwide Class experiencing a fuel shortage, an increase in the

[38] *See, e.g., Colonial Pipeline Co. v. AIG Specialty Ins. Co.*, No. 1:19-cv-00762-MLB (N.D. Ga.), Doc. 114-1, filed April 15, 2021 (Master Services Agreement, section 24, stating that "[t]he validity, construction, interpretation, and performance of the Agreement shall be governed by the laws of the State of Georgia, without regard to conflicts of law principles that would cause the application of the laws of another jurisdiction").

price paid for gasoline, and an inability to sell fuel and other products to their customers.

120. Neither Plaintiff nor the Nationwide Class contributed to the Ransomware Attack.

121. As a direct and proximate result of Defendant's conduct, Plaintiff and the Nationwide Class suffered damages including, but not limited to, a fuel shortage, an increase in the price paid for gasoline, and an inability to sell fuel to their customers, also with attendant burden, inconvenience, distress and anxiety.

122. Defendant's acts and omissions as alleged herein were grossly negligent, willful, wanton, and with reckless disregard for the rights of Plaintiff and the Nationwide Class.

123. As a result of Defendant's negligence and gross negligence, Plaintiff and the Nationwide Class suffered damages, including costs and lost profits incurred as a result of a fuel shortage, an increase in the price paid for gasoline, and an inability to sell fuel to their customers, together with other damages as may be shown at trial.

124. In addition to the above, Plaintiff and the Nationwide Class demand nominal damages.

125. As a direct and proximate result of Defendant's negligence and gross negligence, Plaintiff and the Nationwide Class suffered damages in the aggregate in excess of $5 million.

COUNT II – DECLARATORY AND INJUNCTIVE RELIEF
(On behalf of Plaintiffs and the Nationwide Class)

126. Plaintiff repeats and incorporates the allegations contained in the foregoing paragraphs 1 through ~~121~~ 125 as if fully set forth herein.

127. 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 enjoin and restrain acts, such as here, that are tortious and that create a danger of ongoing harm to interested parties.

128. Defendant's cybersecurity measures were inadequate, and on information and belief continue to be so, jeopardizing the Plaintiff and Class Members' ability to obtain a frere and uninterrupted flow of the product they need.

129. On information and belief, Colonial's cyber insurance will cover the ransom payment which Defendant made to the ransomware attackers.[39] Further,

[39] Jule Pattison-Gordon, US House Interrogates Colonial Pipeline CEO Joseph Blount, June 10, 2021, Government Technology, https://www.govtech.com/security/us-house-interrogates-colonial-pipeline-ceo-joseph-blount?_amp=true (accessed June 18, 2021).

Defendant may be able to seek a tax deduction on the ransom payment. Based on these factors, Plaintiff is concerned that Defendant may lack the incentives to take all the steps necessary to prevent similar cyberintrusions in the future.

130. Pursuant to its authority under the Declaratory Judgment Act, or its general authority to award equitable and injunctive relief, this Court should enter an order finding that Defendant owes a duty to Plaintiff and to the members of the Class to use adequate cybersecurity measures in order to keep the Colonial Pipeline secure and Defendant is obligated to employ reasonable measures to protect its systems and the Pipeline for the benefit of Plaintiff and the Class, and to employ adequate security protocols consistent with law and industry standards.

VIII. DEMAND FOR JURY TRIAL.

Plaintiff hereby demands that this matter be tried before a jury.

IX. PRAYER FOR RELIEF.

WHEREFORE, Plaintiff prays for judgment awarding relief as follows:

A. certifying this action as a class action;

B. appointing Plaintiff as the class representative;

C. appointing below-identified counsel as class counsel;

D. awarding nominal, actual and compensatory damages in an amount to be determined;

E. awarding declaratory, equitable and injunctive relief for the benefit of the

Plaintiff and the Class;

F. awarding restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct to the extent that the evidence may show that such a remedy is warranted;

G. awarding attorneys' fees, costs and expenses, to the extent allowable by law;

H. awarding pre- and post-judgment interest to the extent allowable by law; and

I. affording such other and further relief as this Court may deem just and proper.

Date: June 21, 2021

/s/_____
Gregory John Bosseler
SBN 742496
MORGAN & MORGAN, PLLC
191 Peachtree St., NE
Suite 4200
Atlanta, GA 30306
Phone: (239) 433-6880
gbosseler@forthepeople.com

John A. Yanchunis*
Ryan D. Maxey*
MORGAN & MORGAN COMPLEX BUSINESS DIVISION
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

Joel R. Rhine*
NC State Bar No. 16028
Martin Ramey*
NC State Bar No. 33617
Janet Coleman*
NC State Bar No. 12363
Ruth Sheehan*
NC State Bar No. 48069
RHINE LAW FIRM, P.C.
1612 Military Cutoff Rd., Suite 300
Wilmington, N.C. 28403
Office: (910) 772-9960
Cell: (910) 512-7888
jrr@rhinelawfirm.com
mjr@rhinelawfirm.com
jrc@rhinelawfirm.com
ras@rhinelawfirm.com

Mona Lisa Wallace*
NC State Bar No. 9021
John S. Hughes*
NC State Bar No. 22126
WALLACE AND GRAHAM, P.A.
525 North Main Street
Salisbury, NC 28144
Phone: (704) 633-5244
Fax: (704) 633-9434
mwallace@wallacegraham.com
jhughes@wallacegraham.com

Alexander M. Hall
NC State Bar No. 8295
John F. Green, II
NC State Bar No. 24998
HALL & GREEN, LLP
718 Market Street
Wilmington, NC 28401
Phone: (910) 343-8433
atttyalexhall@gmail.com

**pro hac vice to be filed*

Attorneys for Plaintiff

ClassAction.org