UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

RAMON DICKERSON, individually and on behalf of himself and all others similarly situated,

Plaintiff,

v.

CDPQ COLONIAL PARTNERS, L.P.; IFM (US) COLONIAL PIPELINE 2, LLC; KKR-KEATS PIPELINE INVESTORS, L.P.; KOCH CAPITAL INVESTMENTS COMPANY, LLC; SHELL MIDSTREAM OPERATING LLC; and DOES 1-100, D/B/A COLONIAL PIPELINE COMPANY,

Defendants.

Case No. _____

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff RAMON DICKERSON individually on behalf of himself and all others similarly situated ("Plaintiff"), bring this action against Defendants CDPQ COLONIAL PARTNERS, L.P.; IFM (US) COLONIAL PIPELINE 2, LLC; KKR-KEATS PIPELINE INVESTORS, L.P.; KOCH CAPITAL INVESTMENTS COMPANY, LLC; SHELL MIDSTREAM OPERATING LLC; and DOES 1-100 D/B/A COLONIAL PIPELINE COMPANY (collectively, the "Defendant," the "Colonial Pipeline Company," or the "CPC"), seeking monetary damages, restitution, and/or injunctive relief. Plaintiff makes the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation of their counsel and facts that are a matter of public record.

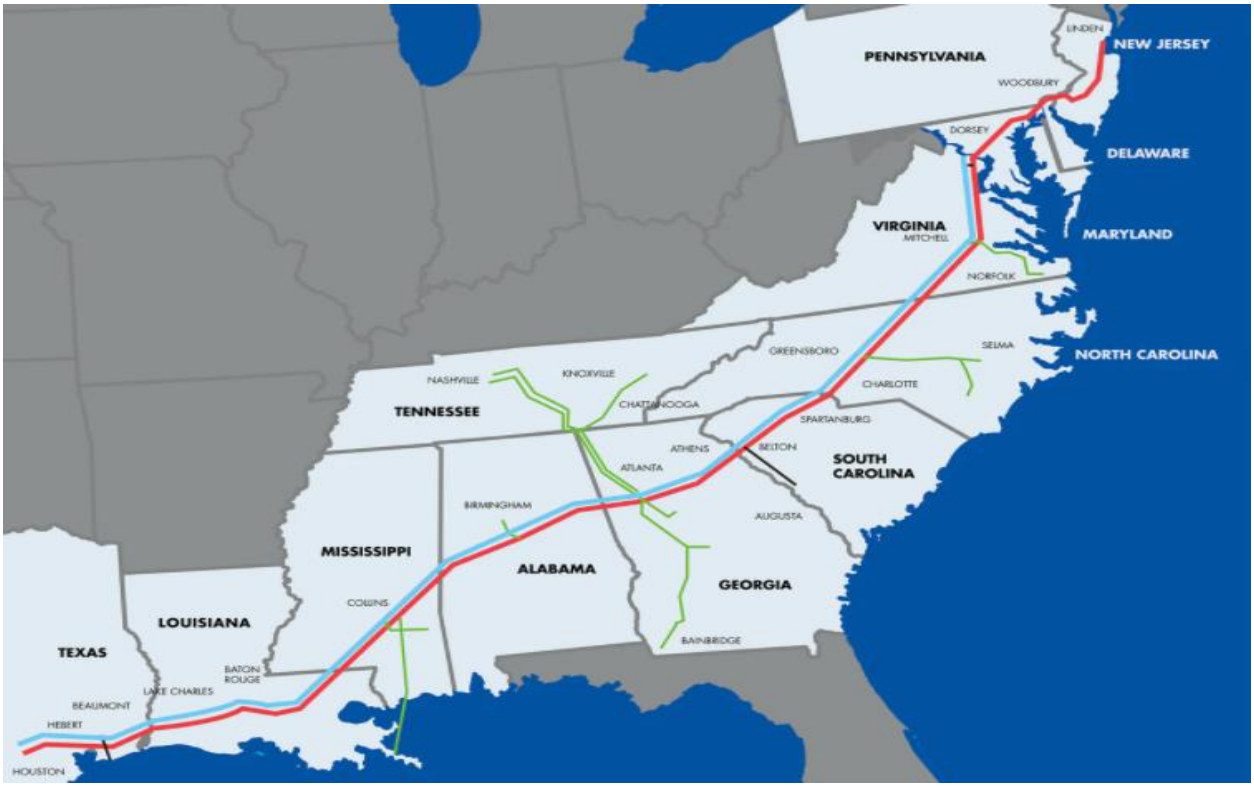
I. INTRODUCTION

1. The Colonial Pipeline ("Colonial Pipeline") supplies the east coast of the United States with gasoline. According to CNBC, "[t]he pipeline is a critical part of U.S. petroleum infrastructure, transporting around 2.5 million barrels per day of gasoline, diesel fuel, heating oil and jet fuel. The pipeline stretches 5,500 miles and carries nearly half of the East Coast's fuel supply. The system also provides jet fuel for airports, including in Atlanta and Baltimore."[1] The Colonial Pipeline, which was

[1] https://www.cnbc.com/2021/05/12/colonial-pipeline-restarts-after-hack-but-supply-chain-wont-return-to-normal-for-a-few-days.html, (last accessed, May 12, 2021).

founded by nine oil companies in 1962, is currently owned by several entities, who collectively do business as the Colonial Pipeline Company; the entities that comprise the Colonial Pipeline Company, according to the Colonial Pipeline's website, includes CDPQ Colonial Partners, L.P., IFM (US) Colonial Pipeline 2, LLC, KKR-Keats Pipeline Investors, L.P., Koch Capital Investments Company, LLC, and Shell Midstream Operating LLC (and, potentially, other entities whose identities will be ascertained at the discovery stage of this litigation).[2]

2. The full breadth, according to the Defendant's website, of the Colonial Pipeline can be seen in the diagram below[3]:



[2] https://www.colpipe.com/about-us/our-company, (last accessed, May 12, 2021).
[3] https://www.colpipe.com/about-us/our-company/system-map, (last accessed May 12, 2021).

3. On May 7, 2021, a massive ransomware cyberattack crippled the Colonial Pipeline's functionality, forcing Defendant to take the pipeline offline – depriving the entire east coast of the normal supply of gasoline needed for the United States economy to fully and properly function.[4] On May 10, 2021, the Federal Bureau of Investigation ("F.B.I.") pinpointed a hacking group called "Darkside" as the perpetrators responsible for the hacking of the Colonial Pipeline.[5]

4. As a result of the Defendant's failure to properly secure the Colonial Pipeline's critical infrastructure – leaving it subjected to potential ransomware attacks like the one that took place on May 7, 2021 – there have been catastrophic effects for consumers and other end-users of gasoline up and down the east coast.

5. The Defendant's unlawfully deficient data security has injured millions of consumers in the form of higher gas prices, and gasoline shortages that exist/existed, due to Colonial's decision to effectively turn off the Pipeline. As a result, Plaintiff brings this action in order to redress the injuries caused to them and the members of the proposed Class due to the Defendant's conduct.

II. JURISDICTION AND VENUE

[4] https://www.cnet.com/news/fbi-says-darkside-hacking-group-responsible-for-pipeline-cyberattack/, (last accessed May 12, 2021).

[5] https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline, (last accessed May 12, 2021).

6. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount-in-controversy, exclusive of costs and interests, exceeds the sum of $5,000,000.00, in the aggregate as there are well over 100 members of the Classes that are known to exist, and this is a class action in which the Plaintiff is from a different State than the Defendant. Namely, Plaintiff Ramon Dickerson is a resident of North Carolina and the Defendant is headquartered in this District.

7. This Court has personal jurisdiction because, among other reasons, Defendant is located in Alpharetta, Georgia.

8. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because the Defendant resides in this District and is a resident of the State of Georgia.

III. PARTIES

9. Plaintiff Ramon Dickerson is a North Carolina resident.

10. Plaintiff Ramon Dickerson purchased gasoline at retail which, as a result of Defendant's conduct, was higher than it otherwise would have been but for the shutdown of the Colonial Pipeline. Plaintiff's purchases took place: on May 7, 2021 in Fayetteville, North Carolina and cost $25; on May 8, 2021 in Fayetteville, North Carolina and cost $15; on May 9, 2021 in Greensboro, North Carolina and cost $20; and on May 10, 2021 in Fayetteville, North Carolina and cost $52.55. As

such, Defendant has caused Plaintiff financial injury that would not have occurred but for the Defendant's conduct alleged herein.

11. Defendant d/b/a Colonial Pipeline Company is an Alpharetta, Georgia-based organization which is comprised of CDPQ Colonial Partners, L.P., IFM (US) Colonial Pipeline 2, LLC, KKR-Keats Pipeline Investors, L.P., Koch Capital Investments Company, LLC, and Shell Midstream Operating LLC.[6] Defendant supplies gasoline by way of a major pipeline, the Colonial Pipeline, and a network of smaller pipelines along the east coast of the United States.

12. Defendant d/b/a Colonial Pipeline Company is a foreign profit corporation which maintains its principal place of business at 1185 Sanctuary Parkway, Suite 100, Alpharetta, Georgia 30009, United States of America.[7] Defendant d/b/a Colonial Pipeline Company is incorporated in Delaware with its registration date listed as October 20, 1961.[8] The officers of the Defendant are listed as Joseph A. Blount, Jr. (Chief Executive Officer), Clayton K. Miller (Chief Financial Officer) and David W. Gray (Secretary).[9] The Defendant's registered

---

[6] https://www.colpipe.com/about-us/our-company, (last accessed May 12, 2021).
[7] https://ecorp.sos.ga.gov/BusinessSearch/BusinessInformation?businessId=566996&businessType=Foreign%20Profit%20Corporation&fromSearch=True, (last accessed May 12, 2021).
[8] *Id.*
[9] *Id.*

agent is CSC of Cobb County, Inc., located in Cobb County, Georgia at 192 Anderson Street SE, Suite 125, Marietta, Georgia 30060, United States of America.[10]

13. Defendant Does 1-100 are subsidiaries and/or affiliates of the d/b/a Defendant Colonial Pipeline Company that may be responsible for the conduct alleged herein. Such parties are named "Does 1-100" pending the discovery portion of this case.

IV. FACTUAL ALLEGATIONS

a. The Colonial Pipeline

14. According to the Defendant's own website, the "Colonial Pipeline is the largest refined products pipeline in the United States, transporting more than 100 million gallons of fuel daily to meet the energy needs of consumers from Houston, Texas to the New York Harbor. Colonial is a value-based energy company, well positioned to provide our services in a cost advantaged, reliable, and environmentally sensitive manner with efficient solutions to meet our customers' needs and the energy demands of the future. We are doing our part to deliver energy that improves lives and keeps the economy moving. At Colonial we are focused on excellence in everything we do. Excellence is woven into our core values. We raise the bar. We exceed the bar. Then we raise it again. But we are more than a pipeline. We are expanding our business to meet the needs of our customers and offer

[10] *Id.*

solutions to meet America's energy demands. Our marine logistics division offers shippers on Colonial an alternative to the Houston Ship Channel by providing water access in the Beaumont Port Arthur area. We develop infrastructure for biodiesel, renewable diesel, and other blending activities, and our 28-million-barrel tank storage capacity helps to maintain a stable supply of energy along our delivery system."[11]

15. The Colonial Pipeline runs up and down the east coast, supplying gasoline to consumers and end-users through its main pipeline, the Colonial Pipeline, and other smaller, ancillary pipelines. The Colonial Pipeline, collectively, "covers more than 5,500 miles and carries more than 100 million gallons of fuel per day, making it the biggest refined products pipeline in the United States[.]"[12] The shipments of gasoline through the Colonial Pipeline move slowly, "at approximately five miles per hour" through its pipes, which means that any delays, interruptions in service, or other issues can cause lasting and residual effects in the market for gasoline on the east coast of the United States.[13]

---

[11] *Id*.

[12] https://www.cnet.com/news/fbi-says-darkside-hacking-group-responsible-for-pipeline-cyberattack/, (last accessed May 12, 2021).

[13] https://www.eia.gov/todayinenergy/detail.php?id=47917, (last accessed, May 12, 2021).

16. According to the Colonial Pipeline Company's website, "[p]revention and detection are the keys to avoiding pipeline emergencies."[14]

b. The Colonial Pipeline's Obligations to Safeguard its Critical Infrastructure

17. One such foreseeable pipeline emergency is exposure to cybersecurity breaches that would cripple the Pipeline's critical function of delivering the most important commodity to the United States economy and sational security.

18. Cybercrime is a well-known risk that should be at the top of any list of potential issues that could occur with respect to infrastructural necessities – like power grids, utilities, and, like in the immediate case, gas pipelines.

19. For example, in 2015, cyberwarfare crippled Ukraine's power grid, and, in 2017, a Russian government-sponsored hacking group called "Dragonfly" or "Energetic Bear" was able to penetrate control rooms' online infrastructures for electrical utilities in the United States in 2017.[15] In 2019, two cities in Florida had their critical infrastructure systems penetrated by ransomware and were forced to pay hackers $600,000 in order to recover from the attack that took place.[16] More

[14] https://www.colpipe.com/our-community/safe-community/emergency-responders/partnering-for-emergency-response, (last accessed, May 12, 2021).
[15] https://www.cnet.com/news/fbi-says-darkside-hacking-group-responsible-for-pipeline-cyberattack/, (last accessed May 12, 2021).
[16] https://www.cnet.com/news/florida-city-will-pay-hackers-600000-to-recover-from-ransomware-attack/, (last accessed May 12, 2021).

recently, in 2020, an Austin, Texas-based company called Solarwinds, which "sells software that lets an organization see what is happening on its networks" was penetrated when "hackers inserted malicious code" into the Solarwinds software platform.[17] That attack, which was credited to Russian intelligence, was able to penetrate and disrupt "multiple [United States government] federal agencies and at least 100 private companies."[18]

20. Each of these high-profile events, along with the scores of well publicized data breaches including Home Depot and Equifax, serve as notice for all critical infrastructures, including the Colonial Pipeline, to adequately protect servers and networks which are used by those infrastructures to supply American citizens with the critical commodities and services they need to function.

21. Additionally, through the United States' federal agency, the Cybersecurity & Infrastructure Security Agency ("CISA"), critical infrastructure systems like the Colonial Pipeline are given training and must complete various exercises consistent with the agency's purpose, which is to work "with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future."[19] The existence and support of an entire federal agency

[17] https://www.cnet.com/news/solarwinds-hackers-accessed-dhs-acting-secretarys-emails-what-you-need-to-know/, (last accessed May 12, 2021).
[18] https://www.cnet.com/news/fbi-says-darkside-hacking-group-responsible-for-pipeline-cyberattack/, (last accessed May 12, 2021).
[19] https://www.cisa.gov/about-cisa, (last accessed May 12, 2021).

dedicated to securing critical infrastructure systems, like the Colonial Pipeline, is further notice to those very same infrastructures about the possibility of cybersecurity attacks like the one alleged herein.

c. The Hack

i. Ransomware

22. According to CISA, "[r]ansomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid. In recent years, ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal, and territorial (SLTT) government entities and critical infrastructure organizations. Malicious actors continue to adjust their ransomware tactics over time, to include pressuring victims for payment by threatening to release stolen data if they refuse to pay, and publicly naming and shaming victims as secondary forms of extortion. Malicious actors engage in lateral movement to target critical data and propagate ransomware across entire networks. These actors also increasingly use tactics, such as deleting system backups, that make restoration and recovery more difficult or infeasible for impacted organizations."[20]

[20] https://www.cisa.gov/ransomware, (last accessed May 12, 2021).

23. With respect to who is at risk for ransomware attacks, CISA states, "[a]nyone with a computer connected to the internet and anyone with important data stored on their computer or network is at risk, including government or law enforcement agencies and healthcare systems or other critical infrastructure entities."[21]

24. With respect to the impact of ransomware, CISA states, "Ransomware can be devastating to an individual or an organization. Some victims pay to recover their files, but there is no guarantee that they will recover their files if they do. Recovery can be a difficult process that may require the services of a reputable data recovery specialist. Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The monetary value of ransom demands has increased, with some demands exceeding $1 million. Ransomware incidents have become more destructive and impactful in nature and scope. The economic and reputational impacts of ransomware incidents, throughout the initial disruption and, at times, extended recovery, have also proven challenging for organizations large and small."[22]

[21] *Id.*
[22] *Id.*

25. With respect to who malicious ransomware actors are, CISA states, "[m]alicious actors can be nation-state actors trying to cause harm to critical infrastructure, or cybercriminals trying to enrich themselves."[23]

26. With respect to mitigations that can be used to resolve the problems caused by malicious ransomware, CISA states, "CISA recommends the following precautions to protect users against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Back up data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when using devices that connect to the Internet."[24]

27. With respect to other best practices against malicious ransomware, CISA states, "[i]n addition, CISA also recommends that organizations employ the following best practices:

[23] *Id.*
[24] *Id.*

- CISA released a guide for parents, teachers and school administrators that provides information to prevent or mitigate malicious cyber actors from targeting kindergarten through twelfth grade (K-12) educational institutions, leading to ransomware attacks, theft of data, and the disruption of learning services.
- Restrict users' permissions to install and run software applications, and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application allow listing to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email 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."[25]

[25] *Id.*

28. At this time, it is not known whether the Defendant employed each of the aforementioned mitigations and best practices in order to adequately secure the Colonial Pipeline from the ransomware attack alleged herein. Nor is it known whether Colonial Pipe could have maintained its fuel transmission operations, even though its computer systems were impacted by the Ransomware and decided to shut down the Pipeline simple to avoid losing some money at the expense of the rest of the economy and national security.

ii. Colonial Pipeline Failed to Meet its Obligations to Protect its Critical Infrastructure

29. At some point on or prior to May 7, 2021, Colonial Pipeline's online systems were penetrated by malicious ransomware as a result of the Defendant's failure to adequately protect its critical infrastructure (the "hack").[26]

30. According to Colonial Pipeline, which reported the hack the next day – on May 8, 2021: "On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems. Upon learning of the issue, a leading, third-party

[26] https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption, (last accessed May 12, 2021).

cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing. We have contacted law enforcement and other federal agencies. Colonial Pipeline is taking steps to understand and resolve this issue. At this time, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation. This process is already underway, and we are working diligently to address this matter and to minimize disruption to our customers and those who rely on Colonial Pipeline."[27]

31. On May 9, 2021, the Colonial Pipeline Company provided an update: "On May 7, Colonial Pipeline Company learned it was the victim of a cybersecurity attack and has since determined that the incident involved ransomware. Quickly after learning of the attack, Colonial proactively took certain systems offline to contain the threat. These actions temporarily halted all pipeline operations and affected some of our IT systems, which we are actively in the process of restoring. Leading, third-party cybersecurity experts were also immediately engaged after discovering the issue and launched an investigation into the nature and scope of this incident. We have remained in contact with law enforcement and other federal agencies, including the Department of Energy who is leading the Federal Government response. Maintaining the operational security of our pipeline, in addition to safely

[27] *Id.*

bringing our systems back online, remain our highest priorities. Over the past 48 hours, Colonial Pipeline personnel have taken additional precautionary measures to help further monitor and protect the safety and security of its pipeline. The Colonial Pipeline operations team is developing a system restart plan. While our mainlines (Lines 1, 2, 3 and 4) remain offline, some smaller lateral lines between terminals and delivery points are now operational. We are in the process of restoring service to other laterals and will bring our full system back online only when we believe it is safe to do so, and in full compliance with the approval of all federal regulations. At this time, our primary focus continues to be the safe and efficient restoration of service to our pipeline system, while minimizing disruption to our customers and all those who rely on Colonial Pipeline. We appreciate the patience and outpouring of support we have received from others throughout the industry."[28]

32. Additionally, on May 9, 2021, the F.B.I. released the following initial statement: "[t]he FBI was notified of a network disruption at Colonial Pipeline on May 7, 2021. We are working closely with the company and our government partners."[29]

33. On May 10, 2021, the Colonial Pipeline Company provided the following update: "Colonial Pipeline continues to dedicate vast resources to

[28] *Id.*

[29] https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks, (last accessed May 12, 2021).

restoring pipeline operations quickly and safely. Segments of our pipeline are being brought back online in a stepwise fashion, in compliance with relevant federal regulations and in close consultation with the Department of Energy, which is leading and coordinating the Federal Government's response. Restoring our network to normal operations is a process that requires the diligent remediation of our systems, and this takes time. In response to the cybersecurity attack on our system, we proactively took certain systems offline to contain the threat, which temporarily halted all pipeline operations, and affected some of our IT systems. To restore service, we must work to ensure that each of these systems can be brought back online safely. While this situation remains fluid and continues to evolve, the Colonial operations team is executing a plan that involves an incremental process that will facilitate a return to service in a phased approach. This plan is based on a number of factors with safety and compliance driving our operational decisions, and the goal of substantially restoring operational service by the end of the week. The Company will provide updates as restoration efforts progress. We continue to evaluate product inventory in storage tanks at our facilities and others along our system and are working with our shippers to move this product to terminals for local delivery. Actions taken by the Federal Government to issue a temporary hours of service exemption for motor carriers and drivers transporting refined products across Colonial's footprint should help alleviate local supply disruptions and we thank our

government partners for their assistance in resolving this matter. Our primary focus continues to be the safe and efficient restoration of service to our pipeline system, while minimizing disruption to our customers and all those who rely on Colonial Pipeline. We appreciate the patience of the traveling public and the support we have received from the Federal Government and our peers throughout the industry."[30]

34. On May 10, 2021, the Colonial Pipeline Company provided an additional update: "Colonial Pipeline is continuing to work in partnership with third-party cybersecurity experts, law enforcement, and other federal agencies to restore pipeline operations quickly and safely. While this situation remains fluid and continues to evolve, the Colonial operations team is executing a plan that involves an incremental process that will facilitate a return to service in a phased approach. We can now report that Line 4, which runs from Greensboro, N.C., to Woodbine, Md., is operating under manual control for a limited period of time while existing inventory is available. As previously announced, while our main lines continue to be offline, some smaller lateral lines between terminals and delivery points are now operational as well. We continue to evaluate product inventory in storage tanks at our facilities and others along our system and are working with our shippers to move this product to terminals for local delivery. Our primary focus

30 https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption, (last accessed May 12, 2021).

remains the safe and efficient restoration of service to our pipeline system, while minimizing disruption to our customers and all those who rely on Colonial Pipeline. We will continue to provide updates as restoration efforts progress."[31]

35. On May 10, 2021, the F.B.I. provided the following update: "[t]he FBI confirms that the Darkside ransomware is responsible for the compromise of the Colonial Pipeline networks. We continue to work with the company and our government partners on the investigation."[32]

36. According to CNBC, Darkside is a "hacker collective" who "intends to carry out more ransom attacks."[33] According to a cybersecurity company called Acronis, Darkside carries out ransomware attacks only against English-speaking countries and "[d]oes not attack hospitals, hospices, schools, universities, non-profit organizations, or government agencies" pursuant to a "code of ethics" that Darkside purports to follow.[34] Seemingly, Darkside takes over networks in order to hold those networks hostage until the party that has been hacked pays a "ransom" which is consistent with how ransomware hacking operates. Below is an image of how the

---

[31] *Id.*

[32] https://www.fbi.gov/news/pressrel/press-releases/fbi-statement-on-network-disruption-at-colonial-pipeline, (last accessed May 12, 2021).

[33] https://www.cnbc.com/2021/05/12/darkside-hacker-group-behind-pipeline-attack-claims-three-new-victims.html, (last accessed May 12, 2021).

[34] https://www.acronis.com/en-au/articles/darkside-ransomware/, (last accessed May 12, 2021).

ransomware ransom note appears once Darkside has taken over a critical network with its ransomware[35]:

37. On May 11, 2021, the Colonial Pipeline Company provided the following update: "Colonial Pipeline continues to make forward progress in our around-the-clock efforts to return our system to service, with additional laterals operating manually to deliver existing inventories to markets along the pipeline. Markets experiencing supply constraints and/or not serviced by other fuel delivery systems are being prioritized. We are collaborating with the Department of Energy (DOE) to evaluate market conditions to support this prioritization. Since our pipeline system was taken offline, working with our shippers, Colonial has delivered approximately 967,000 barrels (~41 million gallons) to various delivery points along

[35] *Id.*

our system. This includes delivery into the following markets: Atlanta, Ga., Belton and Spartanburg, S.C., Charlotte and Greensboro, N.C., Baltimore, Md., and Woodbury and Linden N.J. Additionally, in preparation for our system restart, we have taken delivery of an additional 2 million barrels (~84 million gallons) from refineries for deployment upon restart. Consistent with our safety policies and regulatory requirements, Colonial has increased aerial patrols of our pipeline right of way and deployed more than 50 personnel to walk and drive ~ 5,000 miles of pipeline each day. Actions taken by the Federal Government to issue a temporary hours of service exemption for motor carriers and drivers transporting refined products across Colonial's footprint and actions taken by several Governors to lift weight restrictions on tanker trucks should help alleviate local supply disruptions. This is in addition to the Reid Vapor Pressure wavier issued today by the U.S. EPA that will also help alleviate supply constraints in several states serviced by our system. We would like to thank the White House for their leadership and collaboration in resolving this matter as well as the DOE, PHMSA, FERC and other federal agencies for their ongoing support. Our primary focus remains the safe and efficient restoration of service to our pipeline system, while minimizing disruption

to our customers and all those who rely on Colonial Pipeline. We will continue to provide updates as restoration efforts progress."[36]

38. On May 12, 2021, the Colonial Pipeline Company provided the following update: "Colonial Pipeline initiated the restart of pipeline operations today at approximately 5 p.m. ET. Following this restart, it will take several days for the product delivery supply chain to return to normal. Some markets served by Colonial Pipeline may experience, or continue to experience, intermittent service interruptions during the start-up period. Colonial will move as much gasoline, diesel, and jet fuel as is safely possible and will continue to do so until markets return to normal. As we initiate our return to service, our primary focus remains safety. As part of this startup process, Colonial will conduct a comprehensive series of pipeline safety assessments in compliance with all Federal pipeline safety requirements. This is the first step in the restart process and would not have been possible without the around-the-clock support of Colonial Pipeline's dedicated employees who have worked tirelessly to help us achieve this milestone. We would also like to thank the White House for their leadership and collaboration, as well as the Department of Energy, Department of Transportation, FBI, PHMSA, FERC and other federal, state

[36] https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption, (last accessed May 12, 2021).

and local agencies for their ongoing support. We will continue to provide updates as restart efforts progress."[37]

39. As a result of the foregoing, gas shortages and increased prices for gasoline purchased by consumers and other end-users occurred due to the Defendant's failure to adequately protect their systems from the aforementioned ransomware attack.

iii. Colonial Pipeline - as a Result of a Ransomware Attack Made Possible by Inadequate Cybersecurity Protections - is Taken Offline, Causing Consumer Harm

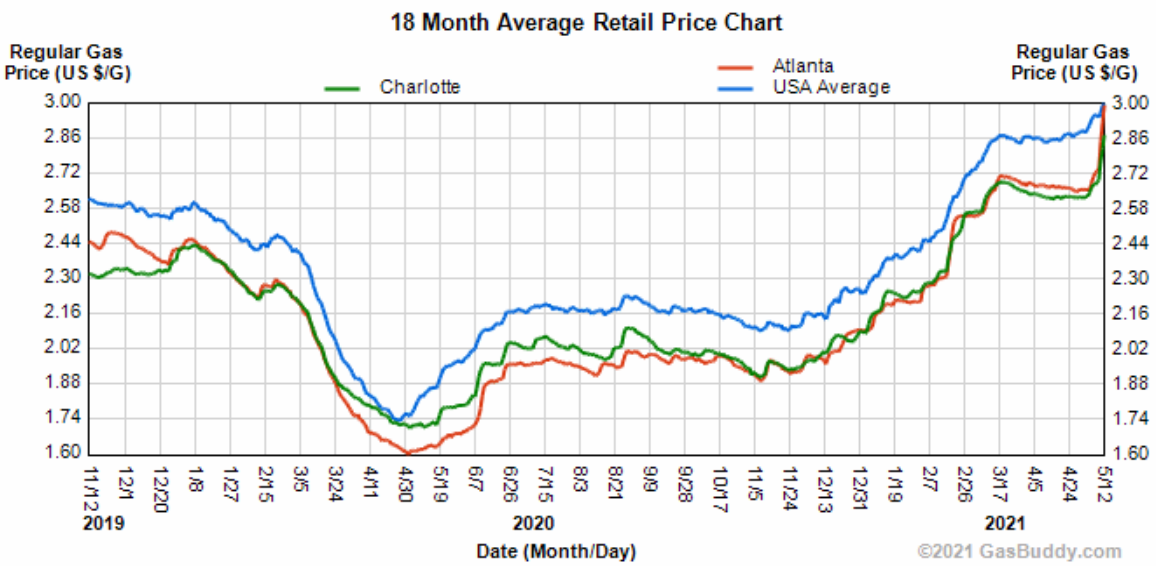
40. As a result of Colonial Pipeline Company's inadequate cybersecurity measures, the Colonial Pipeline was hacked by Darkside.

41. The ransomware hacking of the Colonial Pipeline led the Defendant to take the pipeline (and its network) offline until the ransomware issues could be resolved. This caused substantial disruption to the United States economy and damaged consumers and end-users by way of causing gasoline shortages and exaggerated prices for gasoline in the areas affected by the pipeline's lack of service.

[37] *Id.*

42. According to CNBC, as of May 12, 2021, "68% of gas stations in North Carolina were out of gas… [i]n South Carolina and Georgia 45% of stations [were out of gas], while 49% of stations across Virginia reported outages."[38]

43. The impact on gasoline prices can be seen in the chart included below[39]:



44. For the first time in six years, the average price of a gallon of gasoline in the United States exceeded $3 – and this was due to the Defendant's failure to adequately protect their IT systems and then shut down the Colonial Pipeline. This injured Plaintiff(s) and similarly situated class members, along with the U.S. economy through higher gasoline prices for consumers and end-users.

---

38 https://www.cnbc.com/2021/05/12/colonial-pipeline-restarts-after-hack-but-supply-chain-wont-return-to-normal-for-a-few-days.html, (last accessed May 12, 2021).

39 https://www.gasbuddy.com/charts, (last accessed May 12, 2021).

45. The impact to the price of gasoline can also be seen in the chart below[40]:

NATIONAL AVERAGE GAS PRICES

	Regular	Mid-Grade	Premium	Diesel	E85
Current Avg.	$3.008	$3.325	$3.597	$3.136	$2.534
Yesterday Avg.	$2.985	$3.310	$3.583	$3.125	$2.521
Week Ago Avg.	$2.927	$3.252	$3.527	$3.092	$2.479
Month Ago Avg.	$2.863	$3.199	$3.470	$3.082	$2.465
Year Ago Avg.	$1.854	$2.210	$2.475	$2.418	$1.749

V. CLASS ACTION ALLEGATIONS

46. Plaintiff brings this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "class members."

47. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), and (c)(4) as applicable, Plaintiff proposes the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

> **Nationwide Class**: All entities and natural persons who purchased gasoline from May 7, 2021 through Present and who paid higher prices for gasoline as a result of the Defendant's conduct alleged herein (hereinafter the "Class").

48. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiff proposes state subclasses as necessary or appropriate.

[40] https://gasprices.aaa.com/, (last accessed May 12, 2021).

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

50. Numerosity under Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous and geographically dispersed that individual joinder of all class members is impracticable.

51. Commonality under Federal Rule of Civil Procedure 23(a)(2). There are questions of law and fact common to Plaintiff and class members, which predominate over any questions affecting only individual class members. These common questions of law and fact include, without limitation:

- Whether Defendant failed to adequately protect their servers and systems from malicious attacks, including malware;
- Whether Defendant failed to implement and maintain reasonable security measures, procedures, and practices appropriate to the nature and scope of maintaining critical infrastructure, like a pipeline;

- Whether Defendant truthfully represented the nature of their security systems, including hacker vulnerability;
- Whether Defendant's data security and cybersecurity measures, procedures, and protocols complied with applicable laws and regulations;
- Whether Defendant's data security and cybersecurity measures, procedures, and protocols complied with applicable industry standards;
- Whether Defendant owed a duty to safeguard its systems and servers from malicious hacks;
- Whether Defendant breached a duty to Plaintiff and the Class members to safeguard its systems and servers from malicious hacks;
- Whether Defendant knew or should have known that its data security and cybersecurity measures were deficient;
- Whether Plaintiff and the Class members are owed legally cognizable damages as a result of the Defendant's conduct;
- Whether Defendant was negligent;
- Whether Defendant was negligent per se;

- Whether Defendant failed to provide accurate and complete notice of the hack in a timely manner; and,
- Whether Plaintiff and the Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

52. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of those of the class members because Plaintiff suffered harm in the form of artificially high prices for gasoline at retail due to the inoperability of the Colonial Pipeline due to the hack.

53. **Adequacy of Representation under Federal Rule of Civil Procedure (a)(4).** Plaintiff will fairly and adequately represent and protect the interests of class members, including those from states and jurisdictions where they may not reside. Plaintiff's Counsel are competent and experienced in litigating class actions and were appointed to lead this litigation by the Court pursuant to Federal Rule of Civil Procedure 23(g).

54. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** Defendant has engaged in a common course of conduct toward Plaintiff and the Class members as alleged herein. The common issues arising from Defendant's conduct affecting class members, as described supra, predominate over any

individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

55. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this 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 find that the cost of litigating their individual claim 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.

56. **Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

57. **Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4).** In the alternative, this litigation can be brought and maintained

a class action with respect to particular issues, such as Defendant's liability with respect to the foregoing causes of action.

VI. CAUSES OF ACTION

COUNT I

NEGLIGENCE

58. Plaintiff repeats and reallege all preceding paragraphs, as if fully alleged herein.

59. Defendant's Colonial Pipeline supplies a substantial amount of gasoline – the single most critical commodity to the economy and national security -- to a sizable portion of the United States, including to the states of the Plaintiff named in this Complaint. Defendant makes representations about their reliability with respect to the operational functionality of the Colonial Pipeline.

60. By accepting the duty to deliver a critical commodity and to protect the pipeline in order to keep it running, Defendant had a duty of care to use reasonable means to secure and safeguard its computer systems and gasoline transmission operations. Defendant's duty included a responsibility to implement necessary processes by which it could prevent and/or detect a breach of its computer systems in an expeditious manner, as well as to give prompt notification about the existence of a ransomware attack, in the event one would take place.

61. Defendant additionally owed a duty of care to use security measures consistent with industry standards and other requirements in order to ensure that its systems (and the pipeline itself) were adequately protected and safeguarded and would maintain transmission operations even in the event of computer system failure.

62. Defendant's duty to use reasonable care in protecting its systems (and the pipeline itself) arose because the Defendant is bound by industry standards to protect itself from potential ransomware attacks.

63. Defendant breached the aforementioned duties.

64. Defendant did not use reasonable and/or necessary measures in order to uphold the aforementioned duties – and as a result, the Defendant was hacked by malicious ransomware.

65. Specifically, the acts and omissions committed by the Defendant which were/are negligent include (but are not limited to): (1) failing to adopt, implement, and maintain necessary and adequate security measures in order to protect its systems (and, thus, the pipeline); (2) failing to adequately monitor the security of their networks and systems; (3) failure to ensure that their systems had necessary safeguards to be protected from malicious ransomware; and, perhaps most importantly, (4) failure to ensure that they could maintain their critical fuel transmission operations even in the event of computer system failure.

66. It was foreseeable that the possibility of malicious ransomware attacks would occur with respect to utilities, like pipelines, as malicious ransomware attacks have occurred with respect to other utilities as discussed in this Complaint. Additionally, it was foreseeable that the Defendant's failure to use reasonable measures to protect their computer systems and transmission operations would result in harm to the Plaintiff and the members of the Class.

67. Thus, it was foreseeable that the failure to adequately safeguard the Pipeline's systems would result in injuries to the Plaintiff and the members of the Class.

68. Plaintiff and Class members are entitled to compensatory and consequential damages as a result of the hack.

69. Plaintiff and Class members are also entitled to injunctive relief requiring the Defendant to (1) strengthen its cybersecurity systems and monitoring procedures and (2) to submit future annual audits of those systems and monitoring procedures.

COUNT II

DECLARATORY JUDGMENT

70. Plaintiff repeats and realleges all preceding paragraphs, as if fully alleged herein.

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

72. Plaintiff alleges that the Defendant's data security measures were inadequate. Plaintiff and members of the Class continue to suffer damages at the time of the filing of this complaint in the form of exaggerated prices for gasoline at retail as well as gasoline outages – and any other ancillary damages that could flow as a result of these issues.

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

74. 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 continues to breach this duty by failing to employ reasonable measures to protect its systems (and, thus, the pipeline).

75. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards.

76. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another malicious ransomware hack. The risk of another such hack is real, immediate, and substantial.

77. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued.

78. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another malicious ransomware hack, thus eliminating the additional injuries that would result to Plaintiff and members of the Class.

VII. 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 their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to data and cybersecurity;

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

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including reasonable 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.

VIII. JURY TRIAL DEMAND

Plaintiff hereby demands a jury trial for all claims so triable.

Dated: May 14, 2021

Respectfully submitted,

s/ James Evangelista

James Evangelista
EVANGELISTA WORLEY LLC
500 Sugar Mill Road, Bldg. A, Suite 245
Atlanta, Georgia 30350
Tel.: (404) 600-0945
Email: jim@ewlawllc.com

Harper Segui*
Daniel Bryson*
Rachel Soffin*
Gregory F. Coleman*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
217 Lucas Street, Suite G
Mount Pleasant, South Carolina 29464
Tel.: (919) 500-5000
Fax.: (919) 600-5035
Email: hsegui@milberg.com
dbryson@milberg.com
rsoffin@milberg.com
gcoleman@milberg.com

Jennifer Kraus Czeisler*
Blake Yagman*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: (212) 594-5300
Email: jczeisler@milberg.com
byagman@milberg.com

**Pro Hac Vice forthcoming*

ClassAction.org