BEFORE THE
NEW YORK PUBLIC SERVICE COMMISSION

In the Matter of Cable Company Filings of Annual Financial Reports and Customer Service Reports.	)	Case 09-01904

Cable Telecommunications Association of New York, Inc.
Statement of Necessity Pursuant to Public Officers Law
Section 89(5)(b)(2)

September 2, 2016

Maureen O. Helmer
Laura Mona
Barclay Damon, LLP
Albany, N.Y. 12207
80 State Street
Phone: (518) 429-4220
Email: mhelmer@barclaydamon.com
Email: lmona@barclaydamon.com

Counsel for Cable Telecommunications Association of New York, Inc.

BEFORE THE
NEW YORK PUBLIC SERVICE COMMISSION

In the Matter of Cable Company Filings of Annual Financial Reports and Customer Service Reports.	)	Case 09-01904

Cable Telecommunications Association of New York, Inc.
Statement of Necessity Pursuant to Public Officers Law
Section 89(5)(b)(2)

The Cable Telecommunications Association of New York, Inc., composed of Charter Communications, Inc. ("Charter")[1] and Altice USA ("Altice")[2] (together "CTANY" or the "Companies") respectfully submit this Statement of Necessity in response to the Record Access Officer's ("RAO") letter of August 19, 2016 which provided an opportunity to seek protection of cable outage information provided by the Companies during outage and emergency situations ("Confidential Information") and maintained by the Department of Public Service ("Department").

[1] Note that while much of the information at issue was submitted by Time Warner Cable Inc. ("TWC"), TWC and Charter Communications, Inc. officially merged on May 18, 2016 such that this Statement of Necessity is filed on behalf of the newly merged company, Charter Communications, Inc., as a member of CTANY.

[2] Note that while the information at issue was submitted by Cablevision Services Corporation ("CSC"), CSC and Altice, NV merged on June 21, 2016, such that this Statement of Necessity is filed on behalf of the newly merged company, Altice USA, as a member of CTANY.

The information at issue contains critical infrastructure information, the confidential nature of which is necessary to protect the health and safety of New York's citizens. In addition, the information constitutes trade secret and also commercial information which, if disclosed, would subject the Companies to significant economic and competitive harm.

I. BACKGROUND

On June 30, 2016, Mr. Steve Orr, on behalf of the Democrat and Chronicle, the USA Today Network, the Gannett Co., and himself, requested service outage information as reported to the Commission for the period of 2013 to date by Time Warner Cable, Cablevision, and Charter Communications, Inc. On August 5, 2016, the RAO responded to Mr. Orr's request, finding that a number of filings made under the 09-01904 proceeding,[3] as required by 16 NYCRR § 890.91 which governs installations, outages, and service calls, were responsive to his request with the exception of one TWC filing (Item No. 259 for 2015). The filing at issue was the TWC 2015 Customer Service Annual Report ("Annual Report") filed under a request for confidential treatment on February 1, 2016.[4]

On August 19, 2016 Charter submitted a Statement of Necessity asserting that the Annual Report constitutes a trade secret as well as commercial information which, if disclosed, could result in substantial competitive harm and is therefore exempted from disclosure under the Freedom of Information Law ("FOIL") provisions contained in Public Officers Law ("POL") Sections 87(2)(d) and 89(5)(a)(1). On August 30, 2016, the RAO upheld Charter's request for confidentiality of the Annual Reports.[5]

---

[3] Case 09-01904, *In the Matter of Cable Company Filings of Annual Financial Reports and Customer Service Reports*.

[4] Case 09-01904, *In the Matter of Cable Company Filings of Annual Financial Reports and Customer Service Reports*, Request for exception from disclosure (Feb. 1, 2016).

[5] Case 09-01904, *Records of Service Outages Reported to DPS for 2013, 2014, 2015 and 2016 by Cable Television*

On August 16, 2016, the RAO received a clarification from Mr. Orr for the "location and duration of each outage experienced by cable-TV companies Time Warner Cable, Cablevision and Charter Communications since 2012." By separate letters dated August 19, 2016, the RAO provided each of the Companies "…with an opportunity to assert protection from disclosure pursuant to Public Officers Law§§87(2)(f) and 89(5)(a)(l)(1-a), and the Commission's implementing regulation, 16 NYCRR § 6-1.3, or any other exception that they believe applies." In her letter, the RAO noted the voluntary nature of the information submitted and also advised that she would treat this clarifying request as a separate request from the earlier request which related to the Annual Reports.

This Statement of Necessity explains why the Confidential Information should be excepted from disclosure under FOIL because it (a) constitutes Critical Infrastructure Information; (b) is a trade secret; and (c) constitutes commercial information the disclosure of which would cause the Companies to suffer substantial competitive injury such that it should be exempt from disclosure.

It is important to note that this request for confidentiality pertains to the particular information compiled by Staff pursuant to conversations contemporaneous with outages which is voluntarily provided by the Companies to assist Staff in coordinating recovery efforts. The Companies publicly and routinely communicate information during outages with their customers, affected municipalities, and other stakeholders such as utility companies and critical facilities, and will continue to do so.

Utilities, Time Warner Cable, Cablevision and Charter Communications. Determination of Request for Confidentiality Pursuant to POL §87(2)(d), Determination of the Records Access Officer 16-03, (Issued August 30, 2016).

On the other hand, publication of this particular data could result in a chilling effect on communications during times of emergency and could have broad, adverse impacts on the State's ability to recover from outages of all kinds – gas, electricity, telecommunications, etc. – and therefore could severely hamper the State's ability to protect its critical infrastructure and support the health and safety of its citizens.

Along with this Statement of Necessity, CTANY submits the Declarations of:

- Terence Rafferty, Regional Vice President – Operations for Charter;[6]
- Michael Chowaniec, Vice President of State Government Affairs for Charter;[7]
- Stephen Kramer, Vice President of Network Operations Center for Altice;[8] and
- Matthew Weiss, Senior Vice President, Market Strategy and Insights for Altice.[9]

II. NATURE OF CONFIDENTIAL INFORMATION

During outages, cable providers have voluntarily provided specific and granular information regarding the scope of outages, estimated recovery times, real time assumptions about the root causes of the outages, and potential critical facilities that might be affected. Rafferty ¶¶ 4, 6; Chowaniec ¶¶ 9, 11. This information often involves specific network information, and often includes information related to other providers and impacts on other services such as telecommunications and E911. Rafferty ¶ 4; Chowaniec ¶ 9. Our understanding is that the Department transcribes the information gained from these largely oral communications into a central database. Rafferty ¶ 9. This large database of raw, contemporaneous information

[6] "Rafferty" refers to the August 30, 2016 Declaration of Terence Rafferty.

[7] "Chowaniec" refers to the September 1, 2016 Declaration of Michael Chowaniec.

[8] "Kramer" refers to the September 1, 2016 Declaration of Stephen Kramer, which generally attests to the statements, opinions, and conclusions in the Rafferty Declaration as well as the Chowaniec Declaration.

[9] "Weiss" refers to the September 1, 2016 Declaration of Matthew Weiss, which generally attests to the statements, opinions, and conclusions of the Rafferty Declaration.

which is provided by the Companies but maintained by the Department is what we assume is the subject of this most recent information request by Mr. Orr.

In addition, because major outages often involve impacts on multiple other critical infrastructure segments (electricity, natural gas, steam), much of this Confidential Information database may contain confidential information related to these other industries. *See* Chowaniec ¶ 9, 12.

III. APPLICABLE LAW

A. Critical Infrastructure Information

Under POL § 89(5)(1)(a), "[a] person or entity who submits or otherwise makes available any records to any agency, may, at any time, identify those records or portions thereof that may contain critical infrastructure information ("CII"), and request that the agency that maintains such records except such information from disclosure under POL § 87(2)." POL section 87(2)(f) provides an exception to disclosure of records or portions thereof that "if disclosed could endanger the life or safety of any person."

The Department of Homeland Security has recognized that communications networks are a key element of critical infrastructure:

> The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors. Over the last 25 years, the sector has evolved from predominantly a provider of voice services into a diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems.[10]

[10] U.S. Department of Homeland Security, *Communications Sector*, HOMELAND SECURITY https://www.dhs.gov/communications-sector (last visited Sept. 2, 2016).

The Commission has repeatedly found that network information is exempt from disclosure under FOIL.[11] In addition, "[w]here the request itself contains information which if disclosed would defeat the purpose for which the exception is sought, such information shall also be excepted from disclosure." Critical infrastructure information is defined in POL § 86(5) as "systems, assets, places or things, whether physical or virtual, so vital to the state that the disruption, incapacitation or destruction of such systems, assets, places or things could jeopardize the health, safety, welfare or security of the state, its residents or its economy."

It is important to note that federal regulators consider this type of information highly sensitive and confidential. The Federal Communications Commission ("FCC") maintains a Network Outage Reporting System ("NORS"). On the homepage for that system it notes:

> Obtaining information on communications service disruptions is essential to the FCC's goal of ensuring the reliability and security of the nation's communications infrastructure. Accordingly, the FCC requires communications providers, including wireline, wireless, paging, cable, satellite and Signaling System 7 service providers, to electronically report information about significant disruptions or outages to their communications systems that meet specified thresholds set forth in Part 4 of the FCC's rules (47 C.F.R. Part 4). Communications providers must also report information regarding communications disruptions affecting Enhanced 9-1-1 facilities and airports that meet the thresholds set forth in Part 4 of the FCC's rules. **Given the sensitive nature of this data to both national security and commercial competitiveness, the outage data is presumed to be confidential.**[12] (emphasis added)

While NORS relies on electronically supplied data from the industry, in the instant circumstances, the Staff's input of oral conversations covers the identical type of material and the need for confidentiality is precisely the same.

---

[11] *See e.g.* Case 03-M-1241, *In the Matter of the Facilitation of Intergovernmental Cooperation Regarding the Exchange of Confidential Information*, Policy Statement Regarding The Provision Of Confidential Information To Government Agencies (Issued Sept. 19, 2003).

[12] Federal Communications Commission, *Network Outage Reporting System (NORS)*, FCC.GOV http://transition.fcc.gov/pshs/services/cip/nors/nors.html (last visited Sept. 2, 2016).

With respect to electric infrastructure which shares many of the same characteristics as communications infrastructure, the Federal Energy Regulatory Commission has stated that the "definition of critical infrastructure should encompass all facilities and components of facilities, not just facilities above a certain threshold," and that the size of the project has little to do with the consequences of destruction of a project, "particularly where it is part of a larger overall system."[13] Because the Confidential Information contains information regarding network locations and operations as well as restorative procedures and mitigation measures to prevent future incidents, it could be used by hackers or terrorists to plan and execute an attack on the Nation's utility infrastructure. Therefore, protection of this information is required to avoid jeopardizing public health, safety, welfare and security, and the Confidential Information must be excepted from disclosure.

B. Commercially Sensitive Information

POL Section 87(2)(d) states in relevant part that agencies must deny access to records that "are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise." The Commission provides a similar provision in its regulations at 16 NYCRR 6-1.3(a) wherein the Commission will deny public access to records that are "trade secrets or are maintained for the regulation of commercial enterprise which if disclosed would cause substantial injury to the competitive position of the subject enterprise."

As background, the New York State Appellate Division, Third Department's, recent decision in *Verizon v. Public Service Commission* found that Public Officers' Law § 87(2)(d)

[13] Critical Energy Infrastructure Information, 68 Fed. Reg. 9862 (Mar. 3, 2003).

provides two *alternate* standards, or "tests," to determine whether information should be excepted from public disclosure.[14] As such, information will be exempted from disclosure if it is either (1) a trade secret; **or** (2) if disclosure would result in a likelihood of substantial competitive injury (referred to as the "substantial injury test"). Therefore, if *either* test is met, the information must be excepted from disclosure. It should be noted that many of the trade secret factors also support the substantial competitive injury test. As discussed below, the Companies believe the Confidential Information meets both of these tests.

1. Trade Secret

The Third Department's *Verizon* decision laid out a "two-prong" approach to determine the existence of a trade secret. "First, it must be established that the information in question [1] is a 'formula, pattern, device or compilation of information [2] which is used in one's business, and [3] which gives [one] an opportunity to obtain and advantage over competitors who do not know or use it.'"[15] Each component of this first prong as applied to the Confidential Information based on the supporting declarations are discussed in detail below.

The second prong established in Verizon sets forth the trade secret factors as follows:

> Second, if the information fits this general definition [first prong], then an additional factual determination must be made 'concerning whether the alleged trade secret is truly secret by considering:
>
> (1) the extent to which the information is known outside of the business;
>
> (2) the extent to which it is known by employees and others involved in the business;
>
> (3) the extent of measures taken by the business to guard the secrecy of the information;
>
> (4) the value of the information to the business and its competitors;

[14] *Verizon New York, Inc. v. New York State Public Service Commission*, 137 A.D.3d 66 (3d Dep't 2016).

[15] *Verizon*, 137 A.D.3d at 72.

(5) the amount of effort or money expended by the business in developing the information; [and] (*sic*)

(6) the ease or difficulty with which the information could be properly acquired or duplicated by others.'[16]

These trade secret factors are non-exclusive, and not all factors must be established to prove that a trade secret exists.[17] Many of these same factors are also used in the analysis for whether disclosure would result in substantial competitive injury, as discussed below.

2. <u>Substantial Competitive Injury</u>

The "substantial competitive injury" test evaluates whether disclosure of the confidential information "would be likely to cause substantial injury to the competitive position of the subject commercial enterprise."[18] The Records Access Officer has traditionally relied on the New York Court of Appeals decision in *Encore College Bookstore v. Auxiliary Service Corporation of the State University of New York at Farmingdale*[19] to evaluate whether substantial competitive injury would result from disclosure of the confidential information.[20]

In *Encore*, the Court of Appeals noted that "whether 'substantial competitive harm' exists . . . turns on the commercial value of the requested information to competitors and the cost of acquiring it through other means" and that a showing of actual competitive harm was not required but "[r]ather, actual competition and the likelihood of substantial competitive injury is

[16] *Verizon*, 137 A.D.3d at 72-73.

[17] The Commission has followed this approach in its recent FOIL Determination in Case 14-C-0370, *In the Matter of a Study on the State of Telecommunications in New York State*, Determination of Appeal of Trade Secret Determination, 17 (Issued March 23, 2016) ("Thus, in compliance with the Appellate Division's decision, the entity resisting disclosure 'must make a sufficient showing with respect to each of the six factors,' any trade secret factor that is not established would be deemed to weigh against a finding that the information constitutes a trade secret").

[18] 16 NYCRR § 6-1.3(b)(2).

[19] *Encore College Bookstores v. Auxiliary Serv. Corp.*, 87 N.Y.2d 410 (1995).

[20] *See e.g.* Case 15-M-0388, *Joint Petition of Charter Communications and Time Warner Cable for Approval of a Transfer of Control of Subsidiaries and Franchises, Pro Forma Reorganization, and Certain Financing Arrangements*, Determination 16-02, at 8 (May 4, 2016) ("Determination 16-02).

all that need be shown."[21] As part of assessing commercial value, Encore looked at whether the party opposing disclosure was subject to competition.[22] The *Encore* court also noted that "where [ ] disclosure is the sole means by which competitors can obtain the requested information, the inquiry ends [there]."[23]

Under 16 NYCRR Section 6-1.3(b)(2), the Commission delineated factors to determine whether confidential commercial information "would be likely to cause substantial injury to the competitive position of the subject commercial enterprise."[24]

> Factors to be considered include, but are not necessarily limited to:
>
> (i) the extent to which the disclosure would cause unfair economic or competitive damage;
>
> (ii) the extent to which the information is known by others and can involve similar activities;
>
> (iii) the worth or value of the information to the person and the person's competitors;
>
> (iv) the degree of difficulty and cost of developing the information;
>
> (v) the ease or difficulty associated with obtaining or duplicating the information by others without the person's consent; and
>
> (vi) other statute(s) or regulations specifically excepting the information from disclosure.[25]

While similar, these factors are not the same as the trade secret factors enunciated in the *Verizon* decision, taken from the Restatement of Torts.[26] It should be noted that factors (ii), (iii), (iv), and (v) of the competitive injury analysis overlap with trade secret factors (1), (4), (5), and (6),

---

[21] *Encore*, 87 N.Y.2d at 421 (internal quotes omitted).

[22] *Id.*

[23] *Id.* at 420.

[24] 16 NYCRR § 6-1.3(b)(2).

[25] 16 NYCRR § 6-1.3(b)(2).

[26] Restatement of Torts § 757, comment b; s*ee also, Ashland Mgmt v. Janien*, 82 N.Y.2d 395, 407 (1993).

respectively. As such, much of the information provided in the declarations and in this Statement of Necessity to support that the Confidential Information is a trade secret will also support that the substantial competitive injury test is met.

IV. STATEMENT OF NECESSITY IN SUPPORT OF NON-DISCLOSURE

CRITICAL INFRASTRUCTURE INFORMATION

1. Network Information

During times of outages, a great deal of granular network information is voluntarily exchanged with the Department in order to both keep Staff and the Commission informed as well as to assist in the Department's role in coordinating recovery efforts. Rafferty ¶¶ 6-8; Chowaniec ¶ 11. It is increasingly recognized that future threats to the security of critical infrastructure, such as communications networks, may come as a combination of cyber and physical attacks.[27] Cable networks play a vital and growing role in the backbone of the communications network of this state. As such, knowledge of the particulars of these networks on the part of terrorists could provide information that contributes to a physical/cyber attack which could cripple portions of the state and endanger the life and safety of the state's citizens.

2. Candor During Emergencies

It is vital that those communicating with the Department during outages, especially outages taking place during times of general emergencies, be able to provide unfiltered information with openness, candor and in a timely fashion. If there is a belief that this sensitive information may become public, it will have a chilling effect on these communications.

[27] *See e.g.* Case 03-M-1241,; *see also* Case 14-M-0101, *Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision*, NYS Department Of Public Service Staff Report And Proposal, 2, 24 (April 24, 2014).

Chowaniec ¶ 16. For example, to mitigate risk of disclosure of preliminary information, companies may require higher-level review on the nature and extent of information to be reported, which could delay transmittal or discourage certain communications altogether. Chowaniec ¶ 16.

In addition, since information about probable root causes is being communicated and inputted into the DPS database in real time, there may be significant inaccuracies in portions of the database. Chowaniec ¶¶ 12-15; Kramer ¶ 8. Early surmises by Company personnel may turn out to be inaccurate once further investigation is made, or inconsistent with other critical infrastructure providers. Chowaniec ¶ 14. It is sometimes weeks and even months before an outage is completely understood, but the raw data that is inputted during the event could create confusion on the part of municipalities, other providers and/or the public if released. Chowaniec ¶ 15.

The impact that a chilling effect on communications with Staff could have during times of emergency would clearly have an impact on the health and safety of New York's citizens. After the World Trade Center attacks, the 2003 Northeast power outage, and the numerous hurricanes and super storms the State has faced, DPS played an integral role in helping to coordinate recovery of both electrical and communications systems. A chilling effect on communications by providers of critical services could cripple these efforts.

COMMERCIALLY SENSITIVE INFORMATION

The Confidential Information includes sensitive network information, customer data in affected regions, commercial relationships with other network providers, and various communications protocols utilized by the Companies.

A. The Confidential Information Meets the Trade Secret Standard and Should Be Exempt from Disclosure

1. The First Prong: General Definition of a Trade Secret

i. Formula, Pattern, Device, or Compilation of Information

While the ultimate compilation of the database is accomplished through the expense and efforts of the Department, the inputs to this database constitute a compilation of data by each of the Companies. The confidential information includes data from various offices, call centers, field operations, proprietary forensic instruments and network operations. Rafferty ¶ 9. The information constitutes a "compilation of information" because it consists of a wide array of information that has been derived from a variety of sources including internal company databases and operating systems. Rafferty ¶ 9; Chowaniec ¶ 9. Specific data from these internal sources was extracted in real time during cable outages and relayed unfiltered to Staff contemporaneously with the outage. Chowaniec ¶ 9, 11; Rafferty ¶ 4. The compilation of these various data sources to provide information to the Department clearly meets the first component of the first prong because the data is a "compilation of information."

ii. Used in One's Business

In addition to compiling the information for submission to the Commission, the Confidential Information, in both its granular and aggregated form, is used by the Companies to gauge the reliability of their networks as well as the success rate (and improvement opportunities) of the Companies' recovery efforts to analyze which areas need improvement, and to identify underlying root causes. Rafferty ¶ 10. The Confidential Information is clearly relevant to and used in Companies' businesses.

iii. Which Gives [One] An Opportunity To Obtain An Advantage Over Competitors Who Do Not Know Or Use It

The Confidential Information gives Companies "an opportunity to obtain advantage over competitors who do not know or use it" because the information is based on internal databases that are not publicly known or available (Rafferty ¶¶ 14-15) and provides the Companies with insight into areas of their networks, recovery and customer communications that need improvement or investment (Rafferty ¶ 10). If competitors were allowed access to the data, they would receive a tangible financial benefit, in terms of being spared the cost of independently collecting market data and information about the Companies' network, service, and subscribers. Rafferty ¶ 11. If disclosed, the Confidential Information would provide valuable insights into the Companies' business and operations, and competitors would be able to extract highly confidential business operations information and tailor their own marketing and business strategies to challenge the Companies and use this information in negative marketing campaigns. Rafferty ¶¶ 11-12.

Therefore, the Confidential Information gives each Company an advantage over competitors who do not know the Companies' specific customer communications protocols, reliability vulnerabilities, or resiliency methodology, and allows the Companies to continue to address and improve these issues to mitigate customer attrition and increase service performance.

2. The Second Prong: The Trade Secret Factors

Factor 1: The Extent To Which The Information Is Known Outside Of The Business:

Information which is determined to be important for municipalities and customers during outages, is provided through a variety of methods. However, the detailed forensic information shared with the Department is not otherwise publicly available from the Companies, and to the best of our knowledge is only shared on a "need to know" basis with other stakeholders involved

in an outage and where appropriate with federal regulators and emergency response personnel. Chowaniec ¶ 12; Rafferty ¶ 14.

Factor 2: The Extent To Which It Is Known By Employees And Others Involved In The Business:

Only upper management and relevant, involved employees that have prepared, compiled and/or been involved in reporting the Confidential Information have access to the raw data. Rafferty ¶ 14. After compilation of the information, employees only have access on a need-to-know basis for implementation of the business and operational plans or to plan budgets as well as time and materials for implementation of improvement programs, mitigation measures, or system upgrades. Rafferty ¶ 14. The Companies ensure that the Confidential Information is made internally available only to those who need to access the data to perform their job functions. Rafferty ¶ 14.

Factor 3: The Extent Of Measures Taken By The Business To Guard The Secrecy Of The Information:

After the information is compiled, employees only have access on a need-to-know basis for strategic, facilities and network planning and development and implementation of service quality plans. Rafferty ¶¶ 14-15 . The Companies employ a variety of measures to restrict access to sensitive and confidential information, including the use of password-protected shared document libraries, restricting access to information by job description and category, and also by requiring all employees to participate in annual training to ensure compliance with data protection practices. Rafferty ¶ 15; Weiss ¶ 8-9.

Factor 4: The Value Of The Information To The Business And Its Competitors:

While the Confidential Information cannot be ascribed a precise dollar value, it is indeed very valuable because disclosure would provide competitors an advantage and unique insight for marketing plans to target customers. Rafferty ¶ 16. If competitors were to obtain the

information, they could – and given the opportunity would – use the Confidential Information to develop competitive strategies aimed at the Companies' subscribers and engage in negative marketing campaigns directed at respective Companies. Rafferty ¶ 16. The Companies have committed to significant investments in these areas, and to risk loss of existing or future customers because the Confidential Information were to be made available to competitors who would inaccurately or inappropriately use the Confidential Information would cause substantial injury to the Companies through actual loss of subscribers. Rafferty ¶ 17.

Also, as noted in the CII section above, the FCC has recognized on its NORS website that "Given the sensitive nature of this data to both national security **and commercial competitiveness**, the outage data is presumed to be confidential. (emphasis added)

Factor 5: The Amount Of Effort Or Money Expended By The Business In Developing The Information:

As noted above, the Department bears the expense of compiling the final database of Confidential Information. However, the compilation of the data submitted that constitutes the database and the resources relied upon to have the availability of this data in real time during times of outages is a costly and ongoing endeavor. Rafferty ¶ 18. The Companies have expended millions of dollars and devoted considerable amounts of employee time over the past several years to develop and maintain the data resources relied upon in generating the data that ultimately constitutes the Confidential Information. *Id.* In addition, the annual cost to procure and maintain these data assets is a significant investment for each of the Companies. *Id.*

Factor 6: The Ease Or Difficulty With Which The Information Could Be Properly Acquired Or Duplicated By Others:

While information about the extent and duration of large outages is generally publicly known, the real-time forensics of the root causes of outages could only be guessed at by a competitor. Rafferty ¶ 19.

In sum, the Confidential Information qualifies as a trade secret. The information at issue is a "compilation of information" not otherwise publicly available that was specifically derived by data manipulation conducted by the Companies. If disclosed, competitors would have free access to the same information, and unfairly exploit this information for their own benefit to the detriment and at the economic expense of each of the Companies.

B. Disclosure of the Confidential Information Would be Likely To Cause Substantial Competitive Injury to the Companies

1. Competitive Environment

Robust competition exists in the video business in New York State (Rafferty ¶ 20; Weiss ¶ 6; Kramer ¶ 6), such that each of the companies are subject to "actual competition." Many cable franchises that have been granted to competitors and others in New York and the availability of satellite video service throughout New York State (e.g., DirecTV) and the aggressive marketing of these companies has created a highly competitive cable industry in New York State. Because each Company's network provides a variety of bundled services, including voice, data and video services, negative marketing could take place by competitors in any of these market segments. Rafferty ¶ 21. Disclosure and subsequent misconstruing or mischaracterizing either of the Company's cable service quality, reliability or outage statistics by competitors would have negative market share implications for each of the Companies' voice, video, and data customer bases. Rafferty ¶ 21; Chowaniec ¶ 19.

2. Commercial Value

As presented above in the analysis of trade secret factors four and five, the Confidential Information has tangible value to the Companies that would be severely diminished if the Confidential Information were disclosed. Rafferty ¶ 22. If given free, unfettered access to this information, competitors would use the Confidential Information to develop competitive strategies aimed at the Companies' subscribers and engage in negative marketing campaigns. Rafferty ¶ 22; Chowaniec ¶ 19. The Companies have committed to significant investments in these areas, and to risk loss of existing or future customers because the Confidential Information were to be made available to competitors who would inaccurately or inappropriately use the Confidential Information would cause substantial injury to the Companies through actual loss of subscribers. Rafferty ¶ 22; Chowaniec ¶ 19.

This is particularly true because of the fact that many of the types of providers of services that compete with cable companies do not provide the type of real time outage information that the cable companies provide. Cable providers in New York have previously determined that it is in the best interests of their customers and the communities they serve to provide outage information on a voluntary basis to the Department. Competitors who have not made a similar commitment could, if the Confidential Information is publicly released, misconstrue data contained in the Confidential Information to make comparisons to their reliability without the availability of similar public information to refute such claims. And, as noted above, the data in the Confidential Information database is frequently inaccurate since it contains early surmises about root causes, and thus further susceptible to being misconstrued.

3. Cost of Acquiring Through Other Means

As presented for trade secret factor six, the granular information maintained by the Department could not be recreated by a competitor. Rafferty ¶ 23. The Confidential Information provided by each of the Companies is only available to the Department and to that Company, such that it would be costly, complex, time-consuming, and extraordinarily difficult for others to duplicate. *Id.* Therefore, the only way competitors could access this information in its compiled form would be through disclosure under the Freedom of Information Law ("FOIL") or by expending a significant amount of time and money to develop mere estimates of the Confidential Information from public sources (Rafferty ¶ 23), and as found in *Encore*, because disclosure would be the sole means by which competitors could obtain the Confidential Information, the inquiry should end there and the Report exempted from disclosure.

4. Other Statutes or Regulations

As discussed above, this information is also exempt from disclosure as Critical Infrastructure Information pursuant to POL section 87(2)(f).

V. CONCLUSION

Based on the specific evidence detailed in the declarations of Terence Rafferty, Michael Chowaniec, Matthew Weiss, and Stephen Kramer, the Confidential Information provided by the Companies and maintained by the Department constitute: (a) Critical Infrastructure Information; (b) a trade secret; and (c) confidential commercial information that, if disclosed, would cause substantial injury to each of the Companies. Disclosure of the information could have implications for outage information maintained with respect to other industries regulated by the

Department and therefore have significant adverse effects on the ability to maintain the security of all of the state's critical infrastructure. As such, CTANY respectfully requests that the Records Access Officer grant protection from disclosure of this information.

Dated: September 2, 2016

S/

Maureen O. Helmer
Laura L. Mona
Barclay Damon, LLP
80 State Street
Albany, NY 12207
(518) 429-4220
MHelmer@barclaydamon.com
Lmona@barclaydamon.com
Counsel for The New York Cable Telecommunications Association, Inc.