Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of
Protecting the Privacy of Customer of Broadband and Other Telecommunications Services

WC Docket No. 16-106

COMMENTS OF INCOMPAS

Angie Kronenberg
Christopher L. Shipley
INCOMPAS
1200 G Street NW
Suite 350
Washington, D.C. 20005
(202) 872-5746

May 27, 2016
TABLE OF CONTENTS

I. INTRODUCTION & SUMMARY ................................................................. 1

II. WITH THE NPRM’S FOCUS ON RETAIL MASS MARKET SERVICE, THE FCC SHOULD RECALIBRATE ITS PRIVACY REQUIREMENTS FOR CARRIERS PROVIDING SERVICES TO BUSINESS CUSTOMERS ........... 4

III. HARMONIZATION OF THE CURRENT AND PROPOSED PRIVACY RULES FOR MASS MARKET SERVICES CAN CREATE BENEFITS FOR CUSTOMERS AND TELECOMMUNICATIONS CARRIERS IF THE DISPARITIES CAN BE RECONCILED ......................................................... 7

   a. Harmonization of Current CPNI Rules With the Privacy Notice Requirements ................................................................. 9

   b. Harmonization of Current CPNI Rules With the Customer Approval Requirements for Disclosure of Customer Proprietary Information ........ 11

   c. Harmonization of Current CPNI Rules with Data Security Protections ...... 13

   d. Harmonization of Current CPNI Rules with Data Breach Notification Requirements ........................................................................ 14

IV. CONCLUSION ......................................................................................... 19
Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services

COMMENTS OF INCOMPAS

INCOMPAS, by its undersigned counsel, hereby submits these Comments in response to the Commission’s Notice of Proposed Rulemaking on protecting the privacy of customers of broadband and other telecommunications services.¹

I. INTRODUCTION & SUMMARY

INCOMPAS is the preeminent national industry association for providers of Internet and competitive communications network services. INCOMPAS represents a diverse array of companies. Some of our members provide residential broadband Internet access service (“BIAS”), as well as other mass market services, such as multichannel video programming and voice service to residential customers in urban, suburban, and rural areas. Other members are competitive local exchange carriers (“CLECs”) or new entrants that focus primarily or exclusively on providing communications services to medium-sized and large enterprises, small businesses, local and state governments, including schools and libraries, and non-profits. Our membership includes competitive mobile broadband service providers which offer both mass market and business services. In addition, INCOMPAS represents edge providers that offer

¹ Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Notice of Proposed Rulemaking, WC Docket No. 16-106 (rel. Apr. 1, 2016) (“NPRM”).
services over the Internet, including video services. As a result of our diverse membership, the topic at hand produced a dynamic and diverse discussion among members. It is important to note that the comments we provide today are based on the input we have received from our members. Not every member necessarily agrees with every position we present in these Comments, but our Comments do represent the position of the majority of our membership.

As a supporter of the Commission’s efforts in the Open Internet proceeding and its decision to reclassify BIAS under Title II (a position that INCOMPAS has long held), INCOMPAS lauds the Commission for its efforts to develop a privacy framework for BIAS that safeguards the important confidential information of BIAS subscribers. The application of the privacy provisions of Section 222 of the Communications Act, as amended, is a necessary consequence of the Commission’s reclassification of BIAS as a Title II service. INCOMPAS supports the statutory goals of Section 222, and its member companies have gone to great lengths to ensure that, in the provision of voice service, the private, confidential information of their mass market and business customers is protected through careful adherence to the Commission’s rules on customer proprietary network information (“CPNI”).

Although the Commission seeks comment on the application of its privacy requirements to BIAS services, INCOMPAS focuses its comments solely on questions related to the harmonization of the proposed rules with the Commission’s current CPNI rules. INCOMPAS takes this approach in order to ensure that the impact on the CPNI rules will be targeted and will best promote the public interest and privacy protection objectives of the Commission. In particular, it is imperative that where the Commission’s current rules and policies exempt or

---


3 See 47 CFR § 64.2001, et seq.
provide alternative arrangements with business customers, that such flexibility be maintained. Indeed, INCOMPAS urges the Commission to adopt the distinction it has drawn between mass market and business customers in its definition of BIAS in the larger context of section 222. This will harmonize the treatment of voice and broadband services provided to business customers and allow additional flexibility for companies that are serving business customers to best achieve the protections those customers seek for their broadband and voice services through a negotiated process that is grounded in the framework of Section 222.

The Commission also should carefully consider that its proposed BIAS rules could potentially disrupt the policies and practices of telecommunications providers that already comply with CPNI rules. In each of the major areas that the Commission has identified in its rulemaking—notice, customer approval, securing customer proprietary information (“PI”), and data breach notification—telecommunications carriers are already complying with pre-existing rules. Any harmonization of the CPNI rules with those proposed in the NPRM should balance the Commission’s goals in this proceeding with the practical experience these carriers already have in protecting customer PI. To be clear, harmonizing the rules can be helpful to consumers and the providers that offer both BIAS and mass market voice services—especially because these services typically are purchased in bundles. However, some of the proposed BIAS rules, absent modification, would be more difficult to comply with and would require significant modifications to the current CPNI practices for voice service. Accordingly, INCOMPAS urges the Commission to modify some of its proposed BIAS rules as outlined below before adopting them and harmonizing them with its CPNI rules for mass market customers.
II. WITH THE NPRM’S FOCUS ON RETAIL MASS MARKET SERVICE, THE FCC SHOULD RECALIBRATE ITS PRIVACY REQUIREMENTS FOR CARRIERS PROVIDING SERVICES TO BUSINESS CUSTOMERS

The NPRM presents a unique opportunity for the Commission to consider recalibrating its CPNI rules to better accommodate those carriers that are providing telecommunications services to business customers. As defined, BIAS is a mass market retail service. In 2010, the Commission determined that the term “mass market” should not apply to enterprise service offerings, which it noted “are typically offered to larger organizations through customized or individually negotiated agreements.” The rationale behind this decision stemmed from business customers’ ability to negotiate and contract “for customized services packages” in agreements that “remain in effect for a number of years.”

On the other hand, the Commission’s current CPNI rules apply to both business and mass market voice services. Given that the current CPNI rules were written with mass market consumers in mind, their design is far from optimal for business customers. Telecommunications carriers serving this segment of the market are currently limited in their

---

4 See NPRM at ¶ 29 (proposing to apply the definition of BIAS service used in the 2015 Open Internet Order).
5 47 CFR § 8.11(a).
7 Id. at note 147.
8 See Protecting and Promoting the Open Internet, Report and Order on Remand and Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5610, para. 25 (2015) (“Open Internet Order”).
approaches to compliance with the CPNI rules. The total service approach, for example, hinders the ability of companies to market advanced, IP-based services to business customers that are ready to make the IP-transition by unnecessarily compartmentalizing local, long-distance, and wireless services—services that are routinely sold to enterprise customers as a bundle. Members also report that many enterprise customers are frustrated by the receipt of opt-out notices every two years, and request that they be placed in “permanent” opt-out status.

Enterprise business customers often negotiate service terms with carriers, including privacy and security terms for the services they are purchasing. The Commission’s CPNI rules do not provide the flexibility for carriers to negotiate such arrangements with their customers. Allowing providers of business services to operate within the plain language of Section 222, or at the very least providing far greater flexibility for carriers to negotiate individualized arrangements with their business customers, will ensure that these carriers meet their statutory obligations to protect customer proprietary information while simultaneously opening up their ability to compete and innovate in the areas of privacy and data security and with respect to other services. Ultimately, this approach will enhance the ability of carriers to serve and meet the needs of their customers.

The Commission has previously recognized that business customers are “sophisticated,” and have the capability to ensure that their needs are being met, and as such, additional flexibility is appropriate in the context of its CPNI rules. Under the “business customer...
exemption,” the Commission has permitted carriers to negotiate individualized authentication regimes with business customers that have an account representative. Additional flexibility in meeting the Section 222 obligations for business customers should be considered. INCOMPAS supports an approach of protecting enterprise and business customers’ privacy and proprietary information as such customers have the opportunity to negotiate contracts for services with telecommunications providers served by dedicated account representatives. Moreover, such flexibility will allow telecommunications carriers to better compete on privacy and security in the marketplace and will promote a competitive marketplace that will more effectively meet their security and protection needs of business customers. Accordingly, INCOMPAS proposes that the Commission modify its CPNI rules to exempt enterprise and business customers that have the sophistication and opportunity to negotiate for their telecommunications services, while continuing to require carriers serving these customers to comply with the provisions of Section 222.

If the Commission does not provide a full exemption from the CPNI rules for business customers, it should at a minimum ensure that its rules take into consideration the fundamental differences between mass market and business customers. The Commission’s current proposals to include “customer proprietary information” (“CPI”) and “personally identifiable information” (“PII”) in the list of information that must be protected by carriers is problematic for business negotiated by contract” and that it is unnecessary to extend the carrier authentication rules of CPNI); see also Letter from Karen Reidy, Vice President, Regulatory Affairs, COMPTEL, to Marlene H. Dortch, Secretary, FCC, CC Docket No. 96-115 at 1 (filed Dec. 18, 2006) (explaining that carriers should be allowed to use other reasonable authentication measures developed in consultation with customers as opposed to CPNI safeguards).

11 See 47 CFR § 64.2010(g).
customers. “Individually identifiable” or “readily available biographical information,” as defined in the current CPNI rules, is very rarely made available to providers when dealing with business customers. When setting up a business account, providers typically require businesses to supply a name and business address, as well as contact information for a company representative. The CPNI for businesses collected by providers typically includes records showing the call detail information and the types of services and features customers purchase from their carrier, and INCOMPAS agrees that this is the information that must be protected. It should be noted, however, that the calling number is typically linked to a corporate account, rather than an individual, and providers generally are not informed as to any other details of the customer’s employees or users that make a call. Further, the expectations of privacy that employees have when using a business communication device are significantly different from those of a mass market customer using his or her personal device. Given the significant differences in how carriers handle business customers as opposed to individuals seeking service, including having dedicated account representatives, the Commission would be well served by allowing carriers and business customers to negotiate individualized arrangements within the statutory framework of Section 222.

III. HARMONIZATION OF THE CURRENT AND PROPOSED PRIVACY RULES FOR MASS MARKET SERVICES CAN CREATE BENEFITS FOR CUSTOMERS AND TELECOMMUNICATIONS CARRIERS IF THE DISPARITIES CAN BE RECONCILED

In all major aspects of its current proposal—notice, customer approval, securing customer PI, and data breach notification—the Commission seeks comment on the harmonization of the proposed rules with the current CPNI framework.12 Proper harmonization

could have a number of public interest and economic benefits, both for mass market consumers and for the carriers delivering service. If the Commission commits to harmonizing the privacy rules in a less restrictive manner, and in a way that honors “existing, private sector practices,” telecommunications carriers should be able to, among other things, limit customer “notice fatigue” of privacy requirements by eliminating duplicate or excessive notifications.

Harmonization could also allow carriers to streamline administrative procedures, remove confusing overlap between services, and could provide carriers with the certainty necessary to train sales and customer service personnel to comply with the proposed rules.

The Commission should modify the proposed definition of some terms in the NPRM in order to facilitate that harmonization. In several cases, such as with the definition for “customer PI,” the Commission seeks comment on harmonizing the proposed definition with and applying the new scope of these terms to the pre-existing CPNI framework. Before making such sweeping alterations to the current framework, the Commission must consider that making changes to the definitions will require voice providers to modify their current CPNI policies and practices. Given the burden on carriers to revise their current privacy policies and practices, as well as the potential for customer confusion, the Commission must carefully consider the economic impact the proposed changes will have, particularly if it proceeds to harmonize the BIAS and CPNI rules.

---

13 NPRM at ¶ 10.

14 NPRM at ¶ 59 (“We also seek comment on whether we should harmonize the existing CPNI rules with our proposed rules for broadband providers by adopting one unified definition of customer PI, and on the benefits and burdens of such an approach.”)
a. Harmonization of Current CPNI Rules With the Privacy Notice Requirements

INCOMPAS supports the Commission’s efforts to frame its discussion of privacy protections by using the three fair information practice principles of *transparency*, *choice* and *data security*. With regard to transparency, our member companies have established practices and policies under the CPNI framework that provide their voice customers with “clear, conspicuous, and understandable information about their privacy practices.”\(^\text{15}\) However, the Commission’s proposed definitions of “customer” and “personally identifiable information” has raised concern among competitive telecommunications carriers that these practices may need to be modified or abrogated in order to comply with privacy regulations.

In the NPRM, the Commission defines “customer” as “a current or former” subscriber and also as “an applicant” for BIAS.\(^\text{16}\) This represents a significant expansion from the current CPNI rules, in which a “customer” is defined as “a person or entity to which the telecommunications carrier is currently providing service.”\(^\text{17}\) Specifically, the inclusion of former subscribers and prospective customers creates a disparity with current practices that must be addressed in any harmonization attempt. In practice, this could create industry confusion as to what customer PI should be maintained and could further impact telecommunications providers ability to participate in activities like “win backs” of previous customers. Furthermore, any change to the definition of customer, particularly an expansion like the one proposed, would require carriers to implement new record and document keeping procedures and add to the

\(^{15}\) NPRM at ¶ 82.

\(^{16}\) NPRM at ¶ 31.

\(^{17}\) 47 CFR § 64.2003(f).
number of potential notices being sent to customers, further contributing to “notice fatigue,” lessening the effectiveness of such notices.

Similarly, and particularly with respect to telecommunications carriers serving business customers, the Commission’s proposed definition of “personally identifiable information” is overly broad and would require carriers to make significant adjustments to their customer notice practices. Harmonizing this definition with the current CPNI rules could prove problematic, as the list includes subscriber list information which carriers are statutorily required to disclose “for the purpose of publishing directories in any format.”\textsuperscript{18} The Commission should, at a minimum, ensure that subscriber list information is exempted from the PII definition. Moreover, the proposed definition of “PII” includes a number of identifiable characteristics—such as date and place of birth, mother’s maiden name, biometric information, or information relating to family members, race, religion, and sexual identity or orientation, among others—that simply are not applicable to business customers.

The nature of voice service also makes it extremely unlikely that carriers will be exposed to the types of linked or linkable information described in the NPRM and, consequently, modification of current notice requirements is unnecessary. As further described below, the expansive nature of the information included in the definition of PII, and the failure of the Commission to create any delineation between “sensitive” and “non-sensitive” PII, makes it likely that customers will receive an increased number of breach notifications, leading to customer confusion, notice fatigue, and decreased confidence in their telecommunications service.

\textsuperscript{18} 47 U.S.C. § 222(e).
Harmonizing the proposed rules for providing meaningful notice of privacy policies with the current framework will also require the Commission to take into consideration some of the current practices associated with voice service delivery. Under the proposed rules, in addition to requiring carriers to maintain a privacy policy online at all times, notice of privacy practices must be “made available to prospective customers at the point of sale, prior to the purchase of BIAS, whether such purchase is being made in person, online, over the telephone, or via some other means.” 19 Most carriers currently make their privacy policies continually available on their website, but the existing voice rules do not require companies to provide customers a copy of the policy prior to a retail sale, over the phone, or at the time of purchase. These additional notice requirements are impractical, especially with respect to carriers serving sophisticated business customers. Instead, the Commission should allow these carriers to provide meaningful notice of their privacy policies to their customers using existing practices. This will limit the administrative burden on carriers impacted by the adoption of these rules in areas such as retraining employees to comply with new notice timing rules.

b. Harmonization of Current CPNI Rules With the Customer Approval Requirements for Disclosure of Customer PI

The NPRM seeks comment on whether the Commission should harmonize its proposed framework for when approval is necessary for telecommunications carriers to make use of or disclose customer PI, with the current framework for voice service. 20 In the alternative, the NPRM asks whether the Commission should “revise and modernize” the existing voice

---

19 NPRM, Appendix A, Proposed Rules, § 64.7001(b)(1)-(2) (emphasis added).

20 NPRM at ¶ 108.
framework to include the opt-out/opt-in provisions presented in the proposal.\(^{21}\) Voice providers are permitted under the current rules to disclose CPNI to agents and affiliates to market communications-related services so long as providers give a customer the opportunity to opt-out and stop the sharing of such information.\(^{22}\) This approach allows carriers to offer their customers services that better serve and benefit them as new and innovative services become available.

The proposed privacy rules for BIAS would impose a slightly different set of rules for PI.\(^{23}\) Rather than imposing modified marketing and use restrictions based on the identity of the provider or the type of service at issue, carriers and consumers will be better served by a more flexible regime that recognizes the fact that BIAS is frequently bundled with traditional local, long distance, and even wireless service. Regardless of the approach the Commission takes, any opt-in requirements should be reserved for the use of sensitive data in a way that would surprise consumers. This approach was adopted by the Federal Trade Commission in its 2012 report on privacy protections.\(^{24}\) These approaches would be consistent with the current marketplace and allow telecommunications providers to compete unimpeded in the market.

\(^{21}\) Id.

\(^{22}\) 47 CFR § 64.2007(b).

\(^{23}\) NPRM at ¶ 107.

\(^{24}\) See FED. TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), at viii (recommending that companies should obtain affirmative express consent before collecting sensitive data for certain purposes); NPRM at ¶ 220.
c. **Harmonization of Current CPNI Rules With Data Security Protections**

INCOMPAS agrees with the Commission that “strong data security provisions are crucial to protecting the confidentiality of” customers.\(^{25}\) To that end, telecommunications carriers have successfully developed and implemented security protocols that protect both business and mass market customers. As discussed above, carriers should be provided the opportunity to negotiate individually tailored data security provisions with their customers within the framework provided by the plain language of section 222. At a minimum, however, the Commission should maintain the business customer exemption for authentication regimes under certain circumstances as outlined in Section 64.2010(g).

Under this exemption, those competitive telecommunications providers focusing on serving business customers have developed and implemented robust identification protocols that can be revised as required to meet ever changing technologies and customer requirements. The Commission makes a series of proposals in the NPRM that could affect these contractual arrangements. For example, the current one-for-one user and account system has been successful for telecommunications providers and business customers and should be maintained.

Despite the Commission’s insistence that “adequate disclosure of privacy and security practices is necessary to protect the confidentiality of proprietary information of and relating to consumers,” INCOMPAS member companies assert that they should not be required to disclose their security practices.\(^{26}\) Rather than share this information with the Commission, where the possibility exists that the security practices could be accessed, examined, and breached, our

\(^{25}\) NPRM at ¶ 167.

\(^{26}\) NPRM at ¶ 301.
member companies prefer, and in some cases need, to keep this information out of the public domain. Customers will benefit from their providers refusal to detail their specific security practices and protocols.

Finally, the Commission seeks comment on whether to “require or encourage BIAS providers to use standard encryption when handling and storing personal information.”

Telecommunications carriers currently employ physical safeguards when handling and storing customer information that are unique and appropriate for their own companies and the particular situation (e.g., transmission via a secure private channel, encrypted virtual private network, or shipment via a secure, traceable means). Taking appropriate care in handling and storage of customer data is critical to maintaining customers’ trust and being competitive in this digital age. Encryption is only one component of data security, and as a result of rapid technological development, carriers require the ability to evolve and use the security safeguards that are most applicable to their business and customers’ requirements. The Commission, therefore, should not mandate the encryption technologies or practices that telecommunications carriers use to protect customer PI, especially given that there is no delineation in the NPRM between sensitive and non-sensitive data. The Commission instead would be best served by allowing these carriers to employ and customize the data security program that most effectively services the needs of the company and its customers, as the Commission has traditionally done with their technological network architectures.

d. Harmonization of CPNI Rules with Data Breach Notification Requirements

The Commission seeks comment and guidance on the harmonization of specific data breach notification requirements for telecommunications carriers. While well intentioned, the

27 NPRM at ¶ 216.
proposed rules present an unrealistic and potentially burdensome set of criteria and requirements for alerting customers, law enforcement, and the Commission about actual and inadvertent data breaches.

The proposed rules, if adopted, would lead to a significant increase in data breach incidents and required notifications. The proposed definition of PII is expansive, providing many more opportunities for telecommunications carriers to inadvertently share or make use of linked or linkable information, no matter how difficult it may be to trace back to a customer. Considering the broad scope of information that would qualify as customer PI under the new rules, carriers would be compelled, regardless of the sensitivity of the data, to initiate the data breach notification process should that information be intentionally accessed or disclosed via a good faith mistake that does not result in any actual harm to the consumers.

Compounding that point, the Commission’s proposed definition of “breach” presents a new set of obstacles for telecommunications carriers. The Commission defines “breach” in the NPRM as “any instance in which ‘a person, without authorization or exceeding authorization, has gained access to, used, or disclosed customer proprietary information.’”28 This definition differs from the one currently used under the CPNI framework in that it removes the requirement of intent, which providers have relied upon in developing their breach notification practices.29 Removing the requirement of intent significantly expands the scenarios in which customer notification may be required and the likelihood that notices will be sent to customers when no

---

28 NPRM at ¶ 75.

29 See 47 CFR § 64.2011(e) (defining “breach” as an incident which “has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI”).
actual harm has occurred. For example, a customer service representative who accidentally “gained access” to the wrong customer’s file during a service call, under the proposed rules, would be responsible for a data breach that would require the carrier to begin the notification process. As the Commission points out in the NPRM, customers are susceptible to “notice fatigue” and the proposed rule is likely to increase the number of reportable data breach notifications, without any commensurate benefit for consumers, regulators, or carriers. Indeed, “notice fatigue” is not simply bad for industry, it has very real consequences on consumer confidence in their telecommunications carrier and the services it delivers as well.

To avoid this problem, the Commission must add the intent requirement back into the definition of “breach” in any harmonization of the BIAS and CPNI rules. In the alternative, the Commission should propose language that would exempt providers from notification requirements if the alleged data breach were inadvertent or accidental, and the provider acted in good faith to minimize the threat or harm to customer PI. The customer will be better served by breach notifications that provide detailed information on the sensitive data that was compromised and the possibility of harm. Without an “intent” or “harm” standard, similar to the standard included in many state-level data breach laws,30 customers will not understand the potential impact of breaches in the notification they receive.

The Commission should also limit breach notifications to confirmed instances of misuse of CPNI or customer PI that exceeds a reasonable threshold based on the well-established principle of consumer harm. The Commission may wish to further consider the approach employed by the FTC in which it reviews consumer injury not for trivial or speculative harm, but for monetary or physical harm arising from unwanted economic, health or safety risks. The Commission should also remove the requirement that it be notified of “all data breaches,” including inadvertent breaches in which no consumer is potentially harmed. Telecommunications providers should not be required to notify the Commission when a breach does not give rise to “potentially negative consequences for customers.”

Finally, INCOMPAS encourages the Commission to harmonize its proposed BIAS notification requirements to customers and law enforcement in a manner that is more consistent with the FCC’s current approach, yet provides the flexibility necessary for carriers to service their customers and protect the privacy of their data. The Commission has proposed in the NPRM carriers notify affected customers “no later than 10 days after the discovery of a breach” and in the interim period notifying both the Commission (within 7 days) and law enforcement (within 7 days for breaches of customer PI “reasonably believed to relate to more than 5,000 customers”). Based on our discussions with members, the proposed rules do not provide


31 NPRM at ¶ 76.

32 NPRM at ¶ 234.
enough time for carriers to make data breach determinations conduct an appropriate investigation, identify affected customers, put remedies in place, and send notifications. Most telecommunications services are unlikely to be in a position after seven or even 10 days to have finished a forensic analysis and have the facts regarding a data breach in place to contact the Commission and the affected customers. The current rules provide carriers with seven days, after reasonable determination of a breach, to alert law enforcement, and at a minimum, an additional seven days for law enforcement to conduct an investigation before carriers can notify their customers. Providers of telecommunications service need sufficient time to investigate, prepare notices, train customer service representatives, and perform the necessary systems corrections before notifying customers. If the Commission moves forward with harmonization, it should ensure that the revised rule provides at least the same flexibility offered by the current CPNI rules; however, the Commission is encouraged to align notification with other federal and state laws that allow for longer time frames to ensure that companies have time to provide the best possible information to customers in a timely manner.
IV. CONCLUSION

For the reasons outlined above, INCOMPAS encourages the Commission to adopt a privacy framework for telecommunications carriers that provides the necessary flexibility to meet the statutory obligations of Section 222 as well as the needs of their business customers.

Respectfully submitted,

INCOMPAS

/s/ Christopher L. Shipley

Angie Kronenberg
Christopher L. Shipley
INCOMPAS
1200 G Street, NW
Suite 350
Washington, D.C. 20005
(202) 872-5746

May 27, 2016