

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554**

In the Matter of:

Protecting the Privacy of Customers of  
Broadband and Other Telecommunications  
Services

WC Docket No. 16-106

**REPLY OF TELCORDIA TECHNOLOGIES, INC. D/B/A ICONECTIV**

Telcordia Technologies, Inc.,<sup>1</sup> doing business as iconectiv (“Telcordia” or “iconectiv”), hereby replies to comments filed in response to the Federal Communications Commission’s (“FCC” or “Commission”) Notice of Proposed Rulemaking (“NPRM”) on its proposed privacy rules in the above-referenced proceeding.<sup>2</sup>

Telecommunications carriers are expressly allowed to “us[e], disclos[e], or permit[] access to customer proprietary network information . . . to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services”

---

<sup>1</sup> Since February 14, 2013, Telcordia, a wholly owned subsidiary of Ericsson, has been doing business as iconectiv.

<sup>2</sup> *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, FCC 16-39, WC Docket No. 16-106 (rel. Apr. 1, 2016) (“Privacy NPRM”). Unless otherwise noted, all references to comments in this document are to comments filed on May 27, 2016 in response to the Privacy NPRM.

without first obtaining customer consent.<sup>3</sup> The record in this proceeding confirms that Congressional intent, consumer expectations, and consumer protection require the Commission to allow broadband internet access services (“BIAS”) providers to use and disclose both customer proprietary network information (“CPNI”) and customer proprietary information (“CPI”) *without prior customer consent* to prevent and respond to account takeover (“ATO”) and other fraudulent practices.<sup>4</sup>

Congress intended for carriers to use and disclose even the most sensitive personal data in order to prevent and respond to fraud, including ATO attacks,<sup>5</sup> without first having to seek customer consent. As CTIA notes, imposing a consent requirement before data is used or shared for fraud prevention purposes would have “the perverse result of contravening Congress’s clear intent . . . by inhibiting practices that not only do not result in, but actually prevent, consumer harms such as fraud and identity theft.”<sup>6</sup> Moreover, as Comcast notes, 47 U.S.C. § 222(d)(2) “gives ISPs the right to use or disclose customer information without customer consent as needed to protect carriers and users against *any* fraudulent, abusive, or unlawful use of, or subscription to, broadband services,”<sup>7</sup> including ATO.

---

<sup>3</sup> 47 U.S.C. § 222(d).

<sup>4</sup> See Comments of CTIA at 137-39; Comments of Comcast at 59-60; Comments of the Federal Trade Commission Staff (“FTC”) at 18 (recommending “that the FCC permit BIAS providers and telecommunications carriers to share . . . any . . . information these entities need to locate or identify a particular abusive, fraudulent, or unlawful robocall or live call that traversed their networks”).

<sup>5</sup> iconectiv’s Reply is focused on efforts needed to protect service providers, mobile consumers and the companies they engage with from the harms of ATO. It takes no position on whether the FCC should adopt broadband privacy rules or regulate CPI in the first instance.

<sup>6</sup> Comments of CTIA at 139.

<sup>7</sup> Comments of Comcast at 59 (emphasis in original).

Commenters confirm that this approach not only furthers Congressional intent, it also honors consumer expectations and prevents significant harm. Early and quick interception of fraud protects consumers and businesses—and consumers clearly want this protection.<sup>8</sup> If the FCC were to fail to honor consumer expectations and enact prescriptive regulatory requirements for prior consent in this context, it would inhibit continuous improvement in the ability to implement innovative solutions to protect consumers and to detect, mitigate, and respond to fraudulent activity. For example, as T-Mobile notes, requiring opt-in consent before allowing the use or disclosure of personal data for fraud prevention purposes “itself could impose harm, as the customer simply may not recognize the benefits available [if he or she opts in] and thus may not choose to utilize the [fraud prevention] service.”<sup>9</sup> Moreover, as CTIA explains, ISPs and their fraud partners need to stay flexible to be able to adapt to new and changing threat vectors,<sup>10</sup> and “[b]road information sharing lets companies improve detection, mitigation, and response.”<sup>11</sup>

The sophistication of data analytics is increasing all the time. New data elements are constantly being integrated in innovative ways to detect potential fraud and protect consumers and companies with whom they conduct business. Any regulations that the FCC enacts need to be flexible and allow ISPs to use and disclose CPNI and CPI for fraud prevention purposes whenever it is reasonable to do so.

---

<sup>8</sup> Comments of T-Mobile USA, Inc. at 31 (noting that broadband customers expect their personal data to be used for a wide variety of fraud prevention purposes); *see also* Comments of Cloudmark, Inc. at 3-4; Comments of American Cable Association at 40.

<sup>9</sup> Comments of T-Mobile USA, Inc. at 31.

<sup>10</sup> *See* Comments of CTIA at 137-38.

<sup>11</sup> *Id.* at 140.

This is particularly true in the ATO context. As explained in our Comments filed in this proceeding, ISPs and authorized third party companies providing ATO need timely access to personally identifiable information from mobile broadband providers. Determined fraudsters, by using porting, SIM swapping, and other sophisticated means, can compromise consumer identities and take over accounts to effectuate fraudulent transactions. Once the ATO compromise has occurred, the fraudster will attempt to access customers' services immediately, usually in less than two hours. To prevent ATO and stop fraud after ATO has occurred, iconectiv and other similarly situated parties need real-time and near real-time access to CPNI and CPI from mobile operators.

Thus, if the Commission adopts privacy rules for BIAS services, they should enable ISPs to use both routine and innovative fraud prevention and mitigation practices—including ATO prevention and response services that iconectiv provides—that benefit carriers, customers, and third parties. To do so, the rules must provide for permissionless sharing and use of CPNI and CPI for these purposes.

Moreover, adopting iconectiv's proposed approach will ensure that the FCC's rules are in harmony with the FTC's approach to the use of personally identifiable information for the prevention, detection, and mitigation of fraud. The FTC privacy approach allows sharing and permissionless use of personal data for fraud detection purposes.<sup>12</sup> This time-tested approach to addressing fraud has served consumers well, and the FCC should follow suit.

---

<sup>12</sup> Comments of the FTC Staff at 3-6, 17-19.

## CONCLUSION

The Commission should continue to support the prevention and mitigation of fraud and identity theft. To prevent harm to network operators, their subscribers and the companies with whom they conduct business, any future broadband privacy rules should remain consistent with the intent of section 222(d), by enabling providers to quickly and securely share both CPNI and CPI with their authorized third party fraud prevention partners to protect mobile security identity, and to continuously improve the prevention, detection, and responsiveness to ATO.

Respectfully submitted,

TELCORDIA d/b/a iconectiv



By: \_\_\_\_\_

Its Attorney  
Louise L M Tucker  
Senior Counsel  
444 Hoes Lane  
Piscataway, New Jersey 08854  
(202) 368-5180

Dated: July 6, 2016