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

COMMENTS OF TELCORDIA TECHNOLOGIES, INC. D/B/A ICONECTIV ON PETITIONS FOR RECONSIDERATION

Telcordia Technologies, Inc.,[1] doing business as iconectiv, hereby provides comments on petitions for reconsideration of the FCC's *Broadband Privacy Order*,[2] filed by Oracle Corporation, United States Telecom Association, CTIA, American Cable Association, Association of National Advertisers et al., Competitive Carriers Association, the Consumer Technology Association, ITTA-The Voice of Mid-Size Communications Companies, NCTA-The Internet & Television Association, and Wireless Internet Service Providers Association.[3]

iconectiv takes no position on the merits of these petitions. Rather, it asks the Commission to prevent its consideration of these petitions from casting a shadow over a well-

[1] Since February 14, 2013, Telcordia, a wholly owned subsidiary of Ericsson, has been doing business as iconectiv.

[2] *Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs.*, Report & Order, FCC No. 16-148, WC Docket No. 16-106 (rel. Nov. 2, 2016) ("*Privacy Order*").

[3] *See Protecting the Privacy of Customers of Broadband & Other Telecomms. Servs.*, Public Notice, FCC No. 16-39, WC Docket No. 16-106 (rel. Jan. 17, 2017).

settled and uncontroversial scenario in which carriers can share customer proprietary network information (and any other information that may be protected by Section 222) without consent: "to protect users of [telecommunications] services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[4] The petitions ask the Commission to reconsider its overall approach to regulating telecommunications providers' privacy practices, pursuant to 47 U.S.C. § 222. While iconectiv is not asking the Commission to refrain from reexamining the bulk of its Section 222 rules, a wholesale re-evaluation of the Commission's approach to Section 222 could call into question the FCC's commitment to faithfully implementing the fraud exemption.

To prevent such uncertainty from putting consumers at risk, the FCC should take this opportunity to reiterate the breadth of the fraud exemption without delay.[5] It should clarify that Section 222(d) does not prevent carriers from sharing the CPNI[6] that fraud prevention companies need in order to respond to account takeover fraud. By issuing this clarification, the FCC will avoid creating a roadblock that prevents innovative companies from matching and outpacing fraudsters' sophisticated schemes with even more sophisticated technological solutions.

I. iconectiv can use CPNI to combat account takeover fraud.

Among other security solutions, iconectiv is working to protect the mobile consumers from mobile account takeover ("ATO"). In ATO, a criminal hijacks a phone number (frequently by impersonating a customer and having the number ported to another carrier) and associates it

---

4 47 U.S.C. § 222(d).

5 The Commission could issue such a restatement as an Enforcement FAQ, as part of an order staying or granting reconsideration of the *Privacy Order*, in a public notice, or through a declaratory ruling.

6 Or any other information that the Commission determines Section 222 protects.

with the criminal's device. The thief can then request a password reset for the consumer's email account, bank account, online shopping account, cryptocurrency account, or any other account that uses the customer's phone number to verify the customer's identity. To reset an account password, many companies will send a one-time password to the customer's phone number on the theory that only the customer will have possession of his or her own phone. But since the phone number has been hijacked, that one-time password is sent to the *thief's* phone. The thief can then use the one-time password to gain control over the consumer's account.

The scale and severity of ATO fraud has grown significantly in the past few years. Reports of ATO to the Federal Trade Commission more than doubled between January 2013 and January 2016.[7] According to a recent article in Forbes, criminals who are "incredibly sophisticated and incredibly organized" perpetuate these frauds.[8] They work in coordination and use automated procedures, enabling them to steal quickly. For example, in a recent incident, criminals stole approximately thirty of the same victim's accounts within seven minutes.[9] Even the most tech-savvy and fraud-aware can have difficulty avoiding this type of fraud. As companies protect their customers using mobile identity as a form of multi-factor authentication, the number of accounts vulnerable to ATO will only continue to grow. Consumers, fraud

---

7 Lorrie Cranor, *Your mobile phone account could be hijacked by an identity thief*, Tech@FTC Blog (June 7, 2016), https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief.

8 Laura Shin, *Hackers Have Stolen Millions of Dollars in Bitcoin – Using Only Phone Numbers*, Forbes (Dec. 20, 2016), http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers.

9 *Id.*

prevention companies, companies offering consumer accounts, and carriers *all* stand to gain from improved solutions to combat ATO.

To implement these solutions, however, iconectiv and any other similarly situated fraud prevention companies need access to information protected by Section 222 on an ongoing basis—not a limited subset of information in response to a suspected security incident, or after a consumer realizes he or she needs this protection and grants consent. This is because some of the best indicators of ATO, including calling patterns, qualify as CPNI. And in order to find out what *abnormal* customer behavior is (in the event of a suspected security incident), iconectiv must have access to data demonstrating what *normal* customer behavior is.

Additionally, because ATO is often accomplished through the fraudulent porting of a number from one carrier to another, fraud prevention companies should not face regulatory barriers to accessing data on a carrier's current *or* former customers. Any uncertainty about whether the FCC intends to change its regulatory approach toward the fraud exception could impede fraud prevention provider's and innovator's access to this data and put consumers at risk.

II. Section 222 should not impede fraud prevention companies' access to the data they need to combat ATO.

In this time of general uncertainty about the FCC's overall privacy regulatory approach, the FCC must prevent uncertainty from casting a shadow over the fraud exemption. The FCC should re-iterate that carriers may—at their own option and without prior customer consent—share CPNI with third party fraud prevention partners, even if:

- the party receiving the CPNI is not a carrier,
- the sharing is not limited to individual accounts and occurs on an ongoing basis, rather than only in response to particular instances of suspected fraud,
- other institutions also benefit from the fraud prevention, and/or
- the customer has been ported to another carrier.

Such a clarification would ensure that Section 222 does not impede fraud prevention companies' efforts to combat ATO.

The Commission would be well within its statutory powers to issue such a clarification. The plain language of the statute provides that "[n]othing in [Section 222]," including the provisions dealing with consent, "prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information . . . to protect users of [telecommunications] services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services."[10] Sharing CPNI (and any other information covered by Section 222) in order to prevent or mitigate ATO clearly falls within this exception. Hijacking a phone number involves the fraudulent use of a telecommunications service. A fraudster who uses a hijacked number to access a consumer's private accounts can not only inflict substantial financial harm to the consumer, but also violations of privacy and reputational harms. Preventing and mitigating the effects of ATO protects telecommunications customers. As a result, the plain language of the fraud exemption covers the sharing of CPNI in order to prevent or respond to ATO.

Moreover, Congress wrote Section 222(d)(2) very broadly, choosing not to limit the fraud exemption to specific or narrow circumstances. As such, the fraud exemption extends to carriers' disclosure of the CPNI that iconectiv and other, similarly situated fraud prevention companies need to effectively combat ATO. The statute contains no limits on to whom a carrier can disclose protected information, provided the entity receiving the information will use it for a

[10] 47 U.S.C. § 222(d).

permissible fraud-prevention purpose.[11] Similarly, Congress chose not to limit the exception to specific incident response; as such, it encompasses not only actions taken to combat immediate security threats or threats of fraud, but also ongoing uses and sharing of CPNI related to numerous accounts in order to enhance network and cybersecurity defenses, or address fraud and abuse.[12] Sensibly, Congress chose not to limit the fraud exemption to circumstances where *only* a consumer would benefit, as opposed to both a consumer and the consumer's bank, email provider, or other company serving the consumer. There is no language in the statute suggesting that carriers can share CPNI only if protecting a consumer from fraud has no ancillary benefits.[13] Nor should a phone number being ported from one carrier to another affect the carrier's ability to disclose CPNI pursuant to the fraud exception; there is no statutory limit saying a carrier can no longer protect a customer after his or her number has been ported.[14]

CONCLUSION

iconectiv recognizes that many aspects of the FCC's privacy regulatory regime are currently up for debate. But fraud prevention should not be one of them. Before the Commission takes whatever time it needs to re-evaluate its Section 222 regulations, it should reiterate that carriers can work with fraud prevention partners as needed to combat ATO and

---

[11] *Id.*; *see also Privacy Order* ¶ 214 ("[A]ddressing fraud and abuse [pursuant to 222(d)(2)] may require internal use of customer PI, but also disclosures to third-party researchers and other collaborators.").

[12] 47 U.S.C. § 222(d)(2); *Privacy Order* ¶ 214 ("[We interpret the fraud exception] to encompass not only actions taken to combat immediate security threats, but also uses and sharing to research and develop [1] network and cybersecurity defenses and [2] new techniques and technologies for addressing fraud and abuse.").

[13] 47 U.S.C. § 222(d)(2).

[14] *Id.*

other sophisticated forms of fraud—including new types of fraud that emerge in the coming years.

Respectfully submitted,

/s/ Christopher J. Wright
Christopher J. Wright
Adrienne E. Fowler
Harris, Wiltshire & Grannis, LLP
1919 M St. NW, Eighth Floor
Washington, DC 20036
Counsel to iconectiv

Dated: March 6, 2017