July 19, 2016

Ex Parte

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106

Dear Ms. Dortch:

On July 18, 2016, Chris Drake, Suresh Subramanian, Gary Richenaker and I met separately with three Bureaus to discuss the Commission’s broadband privacy proceeding, including:

1. Charles Mathias, of the Wireless Telecommunications Bureau;
2. Matt DelNero, Daniel Kahn, Melissa Kirkel, and Sherwin Siy of the Wireline Competition Bureau; and

We discussed Comments and Replies filed in the proceeding by iconectiv as reflected in the attached presentation.

During the meetings, we noted iconectiv’s leadership positions in the industry and our work to re-establish trust in telephone number identity and to protect consumers from account take over (ATO). We explained that criminals can impersonate the consumer’s mobile identity and then use that to facilitate the authorization of fraudulent transactions. ATO can result in a violation of privacy, reputational harm, monetary loss to the consumer and generate unauthorized traffic that can have harmful effects on the mobile operator networks.
We noted that the threat landscape for ATO includes the subscriber's financial institutions and other companies with whom they do business. Solving ATO requires timely access to personally identifiable information and we urged the Commission to ensure that its final privacy rules do not impede the ability of mobile operators and authorized third parties to engage in fraud prevention.

We discussed the importance of following the best practices for protecting personal information including retaining only the essential data set and applying obfuscation in order to minimizing the consequences of potential breach. Further, there was discussion that the FCC would be receptive to potential language that would very clearly limit permitted use and also clarify the relationships that should be protected from fraud involving the telephone number identity.

In addition to the above, we answered questions on Antispoofing and Robocalling and provided the attached handout that summarizes mitigation techniques.

Sincerely,

Louise L M Tucker
Privacy, Account Takeover (ATO) & Fraud Prevention

Chris Drake
Natalie McNamer
Gary Richenaker
Suresh Subramanian
Louise Tucker

July 18, 2016
Fast Facts

As the authoritative partner of the communications industry for more than 30 years, our market-leading network and operations management, numbering, registry, messaging and fraud and revenue assurance solutions enable the interconnection of networks, devices, and applications for more than one billion people every day.

Customers including operators, content providers, social networks, enterprises, regulators and more.

Registry services currently processing transactions for more than 2 billion subscribers globally.

Operating the US Common Short Code Registry as of 2016.

16 Number Portability Solutions worldwide and soon the US NPAC.

iconectiv
Industry Leadership

Key Industry Roles

- Board Of Directors & Exec Committee – ATIS
- Board of Directors – SIP Forum
- Chair – ATIS Technology & Operations (TOPS) Council
- Co-Chair – ATIS TOPS IP Testbed Landscape Team
- Co-Chair – ATIS Industry Numbering Committee
- Editor – ATIS/SIP Forum Taskforce IP Routing Architecture
- Member – CTIA Cybersecurity working group
- Member – CTIA Mobile Financial Services Authentication working group
- Member – IETF
ATO and Mobile Identity

- Mobile identity has become a key instrument for authentication, and consequently a key target for fraudsters
- Through account takeover (ATO), criminals impersonate the consumer's mobile identity and then authorize fraudulent transactions
- iconectiv is working on solutions to prevent and detect ATO and re-establish industry trust in a consumer’s mobile identity
Solving ATO

Solving ATO requires timely access to personally identifiable information

- FCC should ensure that its final privacy rules and regulations do not inhibit access to customer data for carriers and their fraud prevention partners
  - §222 explicitly allows carriers to disclose CPNI for fraud prevention purposes
  - rules should also include disclosure of CPI for fraud prevention
  - harmonize with the FTC's privacy approach to addressing fraud
  - clarify ambiguity on what data can be shared with whom

- Companies providing ATO Security solutions need:
  - secure persistent real-time and near-real-time access to CPNI and CPI from mobile broadband providers
  - permissionless use for carriers and authorized third parties, including financial institutions and others involved in business relationships with the consumer

iconectiv
Security and Privacy Plan

- **Access Management**
  for Customer Data Protection

- **Corporate Governance**
  with management oversight by CISO & Chief Privacy Officer

- **Best Practices & Regulatory Alignment**
  - Privacy Protection of Consumer Information & CPNI & CPI
  - FCC Cybersecurity Planning Guide
  - NIST Cybersecurity Framework & Special Publications SP 800 series

- **User Security Management Safeguards**

- **Controlled Data Access Management**

- **Employee Security & Privacy Training**
Why iconectiv

unparalleled leadership and
legacy in global communications

- simple: we make the systems and processes that are extraordinarily complex, comprehensible
- secure: we are trusted with the critical data that makes the world run
- seamless: we simplify information exchange, on a global scale, and make it instantly available

iconectiv
# Existing Robocalling and Spoofing Mitigation Techniques

### ANONYMOUS CALL REJECTION

**Benefit:** Blocks any call not providing Caller ID information

**Limitation:** May block legitimate calls lacking Caller ID information

**Dependent on:** User initiated network service

**Currently available:** Yes

### BLACK LISTING (Service Provider Specific)

**Benefit:** Blocks calls from unwanted numbers

**Limitation:** Spoofers can circumvent black listing by using alternate numbers

**Dependent on:** Network supported application

**Currently available:** Yes

### DO NOT ORIGINATE

**Benefit:** Can make a significant initial impact when implemented in a limited number of large gateways

**Limitation:** Provides no protection against international VoIP originated calls

**Dependent on:** Network supported application

**Currently available:** No

### FILING LEGAL COMPLAINTS

**Benefit:** Consumers are legally entitled to Federal Trade Commission (FTC) protection

**Limitation:** Filing an FTC complaint is only an option after robocalling/spoofing has already negatively affected a consumer

**Dependent on:** User initiated non-network service

**Currently available:** Yes

### HONEYPOTS

**Benefit:** A proactive approach for luring and identifying spoofers

**Limitation:** Requires substantial resources for development, maintenance and ongoing data monitoring

**Dependent on:** Network supported application

**Currently available:** Yes

### MALICIOUS CALL TRACING

**Benefit:** Uses a star code (*) to record call details including source, date and time

**Limitation:** Collected data cannot be utilized until a later time

**Dependent on:** User initiated network service

**Currently available:** Yes

### NATIONAL DO-NOT CALL REGISTRY

**Benefit:** Reduces the instances of unwanted telemarketing calls

**Limitation:** Provides no protection against international VoIP originated calls or deliberate fraudsters

**Dependent on:** User initiated network service

**Currently available:** Yes

### SELECTIVE DISTINCTIVE RINGING

**Benefit:** Allows consumers to assign a specific ringtone to user selected numbers

**Limitation:** Numbers must be pre-selected from a contact list in order to provide notification of incoming calls

**Dependent on:** User initiated network service

**Currently available:** Yes
<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
<th>Limitation</th>
<th>Dependent on</th>
<th>Currently available</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SIMULTANEOUS RING</strong></td>
<td>Incoming calls ring an additional user-defined number simultaneously</td>
<td>Not all switching platforms are capable of providing the feature</td>
<td>Non-network service</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SMART PHONE APPS</strong></td>
<td>Allow precise white lists and black lists to be compiled directly from existing call logs or contact lists</td>
<td>Spoofers can circumvent user compiled lists by using alternate numbers</td>
<td>User initiated smart phone app</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>VERIFIED CALLER ID</strong></td>
<td>Signs and validates the phone number of incoming calls</td>
<td>Only works for end-to-end IP sessions</td>
<td>Network supported application</td>
<td>NO (pending STIR/SHAKEN standards)</td>
</tr>
<tr>
<td><strong>TRACEBACK</strong></td>
<td>Identifies calling source by tracing SS7 signaling data from the terminating service provider back to the originating service provider</td>
<td>Is a time consuming manual process</td>
<td>Network supported application</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>VOICEMAIL SCREENING</strong></td>
<td>Forwards incoming calls directly to a message system within the carrier network for later retrieval by the user</td>
<td>May send legitimate calls to voicemail</td>
<td>User initiated network service</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>WHITE LISTING (Service Provider Specific)</strong></td>
<td>Allows calls only from designated white list numbers</td>
<td>Spoofers can easily implement existing numbers from the Global White List database</td>
<td>User initiated network service</td>
<td>Yes</td>
</tr>
</tbody>
</table>