

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

In the Matter of:)
)
Protecting Consumers from One-Ring Scams) CG Docket No. 20-93
)

COMMENTS OF ICONECTIV, LLC.

iconectiv, LLC. (iconectiv) respectfully submits these comments in response to the Commission’s Notice of Proposed Rulemaking released on April 28th in the above-referenced docket

Introduction and Summary

iconectiv applauds the Commission’s ongoing efforts to protect consumers from the scourge of fraudulent telephone calls. iconectiv has been partnering with the industry to mitigate fraud for over a decade with our fraud protection products covering Wangiri one-ring scams and International Revenue Share Fraud (IRSF), in addition to other threats. iconectiv has been contributing to best practices and threat mitigation for many years as part of the GSMA Fraud and Security Group (FASG) and the Communications Fraud Control Association (CFCA). Recently the GSMA FASG launched a new work item called Validating InterNetwork End-to-End Signaling (VINES) for which iconectiv is both Chair and a contributor. VINES was launched to analyze and make recommendations to address numerous forms of interconnect signaling manipulation, including spoofed calls such as the one-ring scam. iconectiv has been a driving force for the Governance Model and Certificate Management specifications for SHAKEN and recently launched the Policy Administrator serving as the SHAKEN/STIR Call Authentication Trust Anchor.

As a neutral and trusted partner to the industry, the iconectiv comments that follow are focused on important technological and operational considerations based on our experience in this domain. In particular, iconectiv makes the following points:

- Many one-ring scams are perpetrated using domestic re-origination, in addition to calls involving international gateways.
- One-ring scams are, by definition, typically not answered which complicates recognition of these calls if no call record is produced for analysis.
- One-ring scams are perpetrated using unallocated numbers in addition to international toll-generating numbers which are often premium-rate numbers.
- One-ring scams are perpetrated on other mediums in addition to voice (i.e., ringing), including SMS text messages and, potentially, direct (i.e., ringless) voicemail.
- Closer scrutiny is warranted by foreign jurisdictions where parties provide premium-rate off-the-shelf toolkits and also where their clients register to provide such premium rated services based on foreign numbering plans.

Working with the Governments of Foreign Countries ¶10

In the NPRM, the Commission asks how it can work with foreign governments to protect consumers from one-ring scams.¹ iconectiv notes that the one-ring scams which present international toll-generating numbers to American consumers are frequently initiated through platforms that re-originate inside the United States. In such cases, the foreign government and their local telecommunications providers have limits in their ability to ensure such outbound calls do not originate in the first place.

Nonetheless, reducing the opportunity space that can be used for one-ring scams in foreign markets is a worthy objective as countermeasures against this threat. iconectiv suggests that Commission efforts include:

- Reducing originations in foreign markets consistent with ¶10; and,
- Reducing terminations available in foreign markets by increasing the scrutiny of providers of the toolkits that support premium-rate services and those parties offering premium-rate services in those markets.

In terms of the Commission engaging foreign governments to reduce call originations that carry toll-generating calling party information towards the United States, the number ranges for premium-rate numbers are published in each jurisdiction and can be recognized at various points in the voice ecosystem and supply chain, including, but not limited to, service provider fraud management systems, call processing elements, and call analytics engines. However it should be noted that one ring scams, by definition, most often do not get answered as the fraudster terminates the call before that occurs. As a result, it will often be the case that no call record is created from which to draw patterns in certain mitigation platforms.

This may complicate the reduction of originations, yet, the collection and reporting of such calls, whether blocked or not, could provide valuable insight into the global heat map for these scams and the impact inter-governmental efforts to mitigate this scam are having over time. While it may be challenging to recognize a single call as warranting blocking in isolation, the one-ring scam generally casts a very wide net to a large volume of subscribers, and combined with the very short duration, if any duration at all, this is a pattern that is readily discernable with the right systems and numbering intelligence.

In addition, these scams often involve collusion between the one-ring caller and the destination (e.g., premium-rate) service. In these scenarios, unallocated number ranges are also frequently used as the Caller ID to perpetrate a one-ring scam. In that regard, the Commission has granted service providers permission to block incoming calls with malformed or invalid Caller ID² which could be beneficial to explore with foreign governments. Such calls should not require a volume threshold before blocking.

Similarly, SMS text messages with the Caller ID spoofed (known as Sender ID in SMS parlance) are often used to trigger the one-ring scam. This medium is supported separately from the voice service provider infrastructure/components and often originates outside the service provider footprint from messaging and application providers. Still, these originations can be recognized as containing international toll, premium-rate, or

¹ NPRM ¶10.

² R&O and FNPRM, CG 17-59, released 11/11/2017, ¶23

unallocated numbers, and should be included in the intergovernmental dialog. The degree to which one-ring scams leverage ringless voice mail is worth understanding through further study as well.

Beyond monitoring and intervening on the one-ring scam originations, it would be beneficial to reduce the breadth of potential terminations and the resulting ease of monetization. This could include such actions as foreign governments instituting additional rigor before parties are approved to begin operating certain services – in particular those using premium-rate numbers under the foreign governments' national numbering plan. Sophisticated toolkits available on the internet make it incredibly easy to set up and operate a premium-rate service, including SMS broadcast tools to “advertise” the service to a large audience. Stricter verification of such toolkit suppliers and the business entities or individuals applying to offer such a service, could dramatically reduce the number of providers, principally those operating illegally. Stricter verification could include examination of any articles of formation or comparable documents, presence on government control lists, and such. The increased scrutiny could further include reporting on usage patterns periodically throughout the lifetime that they operate such a service.

Incentivizing Voice Service Providers to Stop One-Ring Scams ¶12, 15

The Commission notes in the NPRM that Section 12(b)(4) of the TRACED Act requires it to consider ways to incentivize voice service providers to stop calls that perpetrate one-ring scams from being received by called parties, including consideration of adding identified one-ring scam type numbers to the Commission's existing list of permissible categories for carrier-initiated blocking.³ As noted above, domestic unallocated numbers are already a permissible category for call blocking⁴ and iconectiv supports addition of the following permissible numbering categories that will aid in the blocking of inbound one-ring scams:

- International numbers not allocated in the originating market's numbering plan; and,
- International numbers allocated to premium-rate number ranges in the originating market's numbering plan subject to analytics that suggest reasonable cause to treat such calls as scam calls.

Analytics will be aided by the zero duration that are the very signature for one-ring scam calls and, in addition, the volume of calls from such numbers is generally very high, even in the millions, for an industrial scale one-ring scam campaign. In cases where inbound calls succeed at reaching the consumer, the Commission might consider permitting outbound reply calls from one-ring scam victims to be blocked.

The Commission also seeks comment on additional measures it could adopt to facilitate blocking of one-ring scam calls.⁵ As we note above, the inbound one-ring scams are either zero duration or very short duration by nature which offers better accuracy for identifying them. Also, these destination numbers are often tested by the fraudster on each target network with similarly short durations so outbound test calls to international premium-rate number ranges can be incorporated into the analytics to eliminate false positives. Many mobile network operators are already looking at the sender IDs for one-ring scam signatures amidst their inbound SMS traffic. Lastly, to the extent that one-ring

³ FNPRM, ¶12.

⁴ R&O and FNPRM, CG 17-59, released 11/11/2017, ¶23.

⁵ FNPRM, ¶15.

scams are also perpetrated by leaving ringless voice mail for consumers in order to bypass the inbound call analytics, it may be advisable to scrutinize this vector to detect such scams.

Establishing Obligations on International Gateway Providers ¶20-21

The Commission notes in the NPRM that Section 12(b)(6) of the TRACED Act requires it to consider establishing obligations on international gateway providers that are the first point of entry for these calls into the United States, including potential requirements that such providers “verify with the foreign originator the nature or purpose of calls before initiating service.”⁶ As noted previously, many one-ring scams are not originating from overseas despite appearances to the contrary. It is more cost effective for fraudsters to re-originate on domestic infrastructure within the United States. In those circumstances, there is no international gateway provider in the call path upon which to impose such requirements. This is also true of one-way voice mail and SMS triggered scams which do not use an international gateway provider. Nonetheless, those one-ring scam calls that do originate overseas and pass through an international gateway are worthy of attention.

The Commission also seeks comment on the technical and procedural processes that gateway providers have in place to detect or identify traffic that is likely to be illegal, particularly for calls with foreign origination (e.g., detecting unusual call patterns or large call volumes).⁷ Techniques to mitigate signaling manipulation such as spoofing are under investigation in the GSMA VINES work item. This effort is chaired by iconectiv and International Gateway Providers are contributing to this initiative. It is expected that mitigation recommendations which arise out of VINES will be shared in forums associated with the International Gateway Provider community.

Conclusion

iconectiv encourages the Commission to advance its efforts to protect consumers from scammers through targeted steps and continued enforcement action. With respect to one-ring scams, iconectiv recommends that any Commission action recognize that one-ring calls will often originate on domestic infrastructure, will often be of zero duration and may not produce a call record, will often originate within unallocated number ranges, and often originate in other mediums than voice. Lastly, iconectiv suggests that more scrutiny on parties that operate or support such toll-rated services could reduce the ease by which these attacks can be monetized.

Respectfully submitted,

Glenn T. Reynolds
Head of Government and Industry Affairs
iconectiv, LLC
100 Somerset Corporate Blvd, Bridgewater, NJ 08807
(202) 579-4205
greynolds@iconectiv.com

⁶ NPRM, ¶20.

⁷ NPRM, ¶21.