On August 16, 2013, the Subcommittee on Consumer Protection, Product Safety and Insurance (Subcommittee) requested comments on proposed statutory changes to the Federal Trade Commission (FTC) Act, the Federal Communications Commission's (FCC) enforcement authorities, and the Truth-in-Caller ID Act of 2010. The Subcommittee also requested an analysis of the challenges the telecommunications industry foresees in implementing two robocall screening technologies that were discussed at the Subcommittee's July 10, 2013 hearing, "Stopping Fraudulent Robocall Scams: Can More Be Done?" We were pleased to provide you on September 9, 2013 with comments on the proposed statutory changes, and we are again pleased to provide you with the additional analyses you requested concerning the implementation challenges inherent in the deployment of the technologies developed by Primus Telecommunications Canada, Inc. (Primus Canada) and NoMoRobo. The following analysis is based on the written statements that Primus Canada and NoMoRobo provided the Subcommittee on July 10, publicly available information, and discussions that our association and its members had with representatives of each company following the July 10 hearing.

At the outset, we affirm your observation that as we mark the 10-year anniversary of the National Do-Not-Call Registry (Registry), it is clear that the Registry has been generally effective at limiting calls from legitimate telemarketers, including calls that use a pre-recorded voice. Lawful robocallers, as the term "robocall" is construed by the FCC,[1] are successfully managed through the National Do-Not-Call Registry, and the country can credit Congress, the FCC, the FTC, service providers, telemarketers, and consumers for this success.

Nevertheless, individuals and entities with illegitimate intent ignore the Registry, just as any criminal in any context ignores applicable norms. These individuals and firms may or may not be telemarketing, they may or may not use a prerecorded voice, and they may or may not initiate their calls using autodialers. But they are exploiting inexpensive and widely available software applications and Voice over Internet Protocol (VoIP) technologies to annoy, harass, defraud, and harm individuals and businesses through, as the Chief Technology Officer of Primus, Mr. Matthew Stein aptly described, mass unsolicited calling events. Beyond simply ignoring the Registry, some individuals and firms initiating these events may further employ readily available application technologies for the purpose of fraudulently "spoofing" the telephone numbers that

[1] Notice of Proposed Rulemaking, *Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991*, FCC 10-18 (released January 22, 2010). As Matthew Stein, Chief Technology Officer of Primus Canada explained in his written statement, consumers may have a much more expansive definition of "robocalls" than current legal and regulatory definitions: "Before I proceed, it is important to make clear that we view robocalls and automated telemarketing calls as a subset of mass unsolicited calling, which for convenience I will generally refer to as telemarketing calls throughout my presentation. Our customers have made clear that their view of telemarketing calls does not change if they are greeted by a live person or a recorded message when they pick up the phone." *See* United States Senate Committee on Commerce, Science and Transportation, *Stopping Fraudulent Robocall Scams: Can More Be Done?*, Statement of Matthew Stein, Chief Technology Officer, Primus Telecommunications Inc., p. 1 (July 10, 2013) (*Stein Statement*).

purport to indicate the source of the call and the identity of the calling party, so that intervening communications carriers and end users are misled as to a telephone call's true origin.

Overview of the Primus Canada Technology

Primus Canada is a wholly owned subsidiary of McLean, Virginia-based Primus Telecommunications Group, Incorporated, and operates as a competitive local exchange carrier (CLEC) throughout the Canadian provinces. Primus Canada patented and deployed its network-based Telemarketing Guard to telephone lines serving its residential consumers in Canada as a market differentiator.

Primus Canada's Chief Technology Officer provided this explanation how the Telemarketing Guard service works at the July 10 Subcommittee hearing:

> "When a call is placed to a customer protected by Telemarketing Guard, our system evaluates the call even before the customer's phone is rung. If the system believes, based on feedback provided by our customers, that the caller is likely a telemarketer, the call does not go directly to our customer. Instead, a message is played advising the caller that the customer does not accept telemarketing calls and invites them to press 1 to record their name, so that their call can be announced to the party they are calling. After the caller records their name, similar to leaving a voicemail, the system calls our customer and advises them that they have received a potential telemarketing call and plays the recording provided by the caller. The customer then has the choice to accept the call, refuse the call, or send the call to voicemail if available. In fact, customers often decide to ignore the call altogether without even having to answer the phone as the caller ID will display the name "Telemarketing Guard" along with the original caller's phone number."[2]

Although Primus Canada's parent company, Primus Telecommunications Group based in Virginia, offers a US-based VoIP service, it does not currently offer its Telemarketing Guard service to US consumers.[3]

Overview of the NoMoRobo Technology

NoMoRobo is a third-party, cloud-based application that in limited instances can be acquired by consumers for use with their underlying voice service. By utilizing cloud-based voice network and virtual server technologies, NoMoRobo interrogates all phone calls that reach its server from the subscriber's underlying phone service. The NoMoRobo service is entirely dependent on the availability of "simultaneous ring" as part of a consumer's suite of voice communications service features. The NoMoRobo service launched on September 30, 2013.

---

[2] *Stein Statement*, p. 2.

[3] *See*, Lingo website, *Features* (available at: http://www.lingo.com/voip/features/features.jsp) (visited October 9, 2013). The Lingo VoIP website identifies several "privacy and safety" features available with its service, including Caller ID, Anonymous Call Rejection, and Do Not Disturb. Many of these services are identical to those offered by USTelecom members.

Aaron Foss provided the Subcommittee with the following written statement of NoMoRobo technology:

> "In real-time, Nomorobo analyzes the incoming Caller ID and call frequency, across multiple phone lines. If it detects a robocaller, the call is automatically disconnected. All of this happens before the consumer's phone rings.
>
> As each call is analyzed, a blacklist of robocallers is continually updated. The system is actually built using the same technology that the robocallers are using, allowing it to scale, inexpensively, to handle millions of calls. The more calls that come into the system for analysis, the better the algorithm works.
>
> Nomorobo works on land lines, voice-over-IP and cell phones on all of the major carriers and does not require any additional hardware or software. All that is required by the consumer is a simple, one-time setup, enabling a free feature called simultaneous ring."[4]

The NoMoRobo "block list"[5] is developed and maintained through three sources: 1) regularly scheduled updates from the Do-Not-Call Complaint database maintained by the FTC and some states; 2) phone numbers identified by NoMoRobo subscribers; and 3) the blocking of all phone numbers associated with specific entities as determined by NoMoRobo using its own criteria. In any instance where an incoming phone number appears on the NoMoRobo block list, that call is intercepted by the NoMoRobo system before other phone numbers on the simultaneous ring path can be answered.

General Limitations of the Primus and NoMoRobo Technologies

Both the Primus and NoMoRobo technologies are call-blocking technologies and both technologies are list-based – meaning that both technologies are designed to block a specified list of telephone numbers. A currently unresolvable limitation of these technologies is that they generally cannot identify a "spoofed" call. When a legitimate number is repeatedly spoofed, it is likely to be added to a "block list," blocking even legitimate calls from that number. And if a robocaller randomly spoofs many different numbers, the "block list" technology will fail to identify and block robocalls – "false negatives." Note that both of these cases are also likely to cause "false positives" – the inclusion of legitimate numbers in "block lists," and the subsequent blocking and delay of even legitimate calls from these numbers. Perversely, the more that block list based solutions are adopted in an environment where it is easy to spoof telephone numbers, the more likely robocallers are to spoof legitimate phone numbers in order to evade block list

[4] United States Senate Committee on Commerce, Science and Transportation, "Stopping Fraudulent Robocall Scams: Can More Be Done?" Statement of Aaron Foss, p. 1 (July 10, 2013) (*Foss Statement*). For the reasons described in footnote 20 below and the accompanying text, USTelecom believes Mr. Foss's testimony, while technically accurate, tends to convey a vastly oversimplified picture of NoMoRobo's technological limitations and availability. In point of fact, the service is currently available only to those consumers using a VoIP voice platform.

[5] USTelecom uses the term "block list" to describe the list of telephone numbers to be blocked.

based defenses. Therefore, neither technology can be widely deployed in U.S. carrier networks for two related reasons – the general legal prohibitions against call blocking to which U.S. carriers are subject, and the inherent vulnerability of these technologies to telephone number spoofing.

As Henning Schulzrinne, the FCC's Chief Technology Officer, explained at last year's FTC Robocalling Summit, individuals and entities who ignore the National Do-Not-Call Registry or who spoof calling party telephone numbers:

> "leverage the ability to access Voice over IP services. The two advantages that [VoIP services] offer are distance and insensitivity. You can be anywhere in particular outside the jurisdiction where you might not face prosecution and you can do that at a very low cost. VoIP makes it much easier to hide the true identity of the call and insert caller identity information of somebody else, either to obscure your origin with no particular intent to hide behind somebody else simply for all calls to appear to come from different numbers so that you cannot block those easily. Or even more nefariously, pretend to be an organization that you trust, such as a bank, a government agency, Social Security Administration, a doctor's office, or other entity where the call[ed] person is more likely to both pick up the phone and believe, at least initially, the sales pitch."[6]

Dr. Schulzrinne went on to state, "What can consumers do? *Unfortunately. . . there's not much you can do because the basic problem is you don't know where the call really came from. . .* About the only viable option that you do have and the consumers do have is to file a complaint with donotcall.gov because that at least provides more data and more input to law enforcement."[7]

U.S. carriers' own call screening services are subject to the same challenges, as is their ability to implement network based blocking services. This vulnerability is compounded by their obligation, as common carriers, to complete telephone calls. This is why U.S. carriers are leading the way to find a long-term solution to the basic problem of ensuring that individuals and businesses can trust that the telephone number associated with an incoming call accurately represents the true source of that call.

I. The Current Legal Framework Generally Prohibits Carriers from Blocking Calls.

USTelecom's member companies, unlike many entities that are able to provide voice communications services over various platforms, or the individuals and entities that are responsible for generating fraudulent telephone calls, are subject to legacy common carrier regulation and enforcement of that regulation by the FCC. On repeated occasions, the FCC has concluded that call blocking is an unjust and unreasonable practice under section 201(b) of the Communications Act of 1934, as amended (the Act).[8] In general, in a series of decisions dating

[6] FTC Robocall Summit Transcript, *Robocalls: All the Rage – an FTC Summit*, Presentation of Henning Schulzrinne, Chief Technology Officer, FCC, October 18, 2012, p. 21-22.

[7] *Id*. (emphasis added).

[8] 47 U.S.C. § 201(b).

back 25 years,[9] the FCC has stated that its existing precedent provides that "no carriers . . . may block, choke, reduce or restrict [telecommunications] traffic *in any way*."[10] In its November 2011 order reforming universal service and intercarrier compensation, the Commission also made clear that the broad prohibition on call blocking applies to VoIP calls that are originated or terminated on the Public Switched Telephone Network (PSTN).[11]

Indeed, so great is the concern about this issue that on December 3, 2012, 36 Senators sent a letter to the FCC encouraging it to aggressively pursue voice service providers who are not completing calls to consumers and businesses in rural America. As recently as last month, the FCC emphasized that the blocking of telephone calls is "antithetical" to the "seminal objective" of the Act.[12] It concluded that call blocking poses a "serious threat" to "'the ubiquity and seamlessness'" of the network, and absent a general ban on call blocking, "callers might never be assured that their calls would go through."[13] If a carrier engages in prohibited call-blocking activities, the FCC can take appropriate enforcement actions, including cease-and-desist orders, forfeitures, and license revocations. Section 503(b)(2)(B) of the Act authorizes the FCC to assess a forfeiture of up to $150,000 for each violation or each day of a continuing violation, up to a statutory maximum of $1,500,000 for a single act or failure to act.

Both the Primus Canada and NoMoRobo technologies constitute a form of call blocking, since they effectively "reduce or restrict" telecommunications traffic. The FCC is unequivocal in its strict oversight in ensuring the unimpeded delivery of telecommunications traffic. While a non-carrier such as NoMoRobo is not subject to these statutory mechanisms, USTelecom members are prohibited from blocking telephone traffic. And while we are not aware of the specific rationale for the failure of Primus Canada's U.S. parent company to offer Telemarketing Guard in this country as part of its CLEC service, perhaps this legal impediment accounts for at least part of that explanation.

Carriers can and do block harassing and annoying telephone traffic at their end-user customer's request and with their consent, but they are only able to implement such measures for a discrete set of specific phone numbers. [14] In short, in today's world call blocking by carriers is a last

---

[9] Memorandum Opinion and Order, *Blocking Interstate Traffic in Iowa*, FCC 87-51, 2 FCC Rcd 2692 (1987).

[10] *See, e.g.*, Report and Order and Further Notice of Proposed Rulemaking, *Connect America Fund*, 26 FCC Rcd 17663, FCC 11-161, ¶ 734 (released November 18, 2011) (*USF Order*) (emphasis added); *see also*, Declaratory Ruling and Order, *Policies and Rules Concerning Operator Service Providers*, DA 13-1990, ¶¶ 8 – 9 (released September 26, 2013) (*Operator Service Order*); Declaratory Ruling, *Developing an Unified Intercarrier Compensation Regime*, DA 12-54 (released February 6, 2012) (*FCC Declaratory Ruling*).

[11] *USF Order*, ¶ 973.

[12] *Operator Service Order*, ¶ 8.

[13] *Id*.

[14] *USF Order*, n. 2038 (stating that the FCC's general prohibition on call blocking had no effect on the "right of individual end users to choose to block incoming calls from unwanted callers."

resort remedy, done only at the specific request, and with the express consent, of the end user customer or, in even narrower circumstances, to protect the rights and property of the carrier.

II. Technological Concerns and Limitations with Primus and NoMoRobo Measures

A. There are Limitations and Risks to Utilizing a Block List

There are several technological limitations that will hinder the commercial services discussed during the July 10 hearing. Both NoMoRobo and Primus rely extensively on the use of "block lists" – and in the case of NoMoRobo, it relies *exclusively* on block lists. Block lists contain a universe of phone numbers that have been identified as originating robocalls. These lists can be populated based on customer feedback (*e.g.*, through a prompt or portal), or through data provided from the Do-Not-Call list maintained by the FTC and some states. The NoMoRobo technology receives updated information every two weeks from the FTC's Do-Not-Call Complaint database, and the Indiana Attorney General has provided the company with telephone numbers to block.[15] In addition, the NoMoRobo technology blocks outright the phone numbers from a select group of entities identified by NoMoRobo – regardless of whether the phone numbers appear on the FTC's Do-Not-Call Complaint database, or have been provided by consumers through available mechanisms.

1. Block List Technologies are Easily Circumvented

The fundamental challenge carriers and consumers face is that the telephone number delivered with each call – whether initiated by a human or a machine – is the only way for a carrier or an end user to identify the purported calling party. This telephone number is easily hidden, disguised, or deliberately spoofed at origination and through call delivery, even though federal law prohibits such activity.[16] Consumers may see a calling party's number that they trust – a local school, service provider, government agency, etc. – and answer the phone only to hear a pre-recorded message on the other end. The authenticity and reliability of the telephone number associated with an incoming telephone call is increasingly called into question, and inauthentic or "spoofed" telephone numbers are fully capable of defeating today's consumer and carrier controls.

Therefore, because any phone number can be easily spoofed, technologies that rely extensively on the use of block lists can be easily circumvented. In fact, the FCC's own chief technologist recently concluded that only by comprehensively addressing spoofing can the number of illegal

---

[15] *See*, IncNow website, Emma Koch, *Zoeller Partners With Businesses To Help Block Unwanted Calls*, August 16, 2013 (available at: http://www.indianasnewscenter.com/news/local/Zoeller-Partners-With-Businesses-To-Help-Block-Unwanted-Calls-219930711.html) (visited October 10, 2013).

[16] Truth in Caller ID Act of 2009 (P.L. 111-331).

robocalls be reduced.[17] Further, while robocallers currently utilize only a small universe of phone numbers to conduct their operations, they are increasingly randomizing the phone numbers that they employ in their calling schemes.

Once a system relying on block lists is extensively deployed, our previous experience suggests that robocallers can easily and rapidly transition to randomized numbers in order to circumvent such protections. In fact, the widespread deployment of a technology based on block lists could have the perverse effect of quickly nullifying any protections, while also making robocallers more difficult to identify, as robocalling adversaries stay one or more steps ahead of reactive technologies.

2. Widespread Deployment of Block List Technologies is Inherently Risky

Given the ease of telephone number spoofing, the use of block lists on a large scale is inherently risky since robocallers using randomized numbers could very easily spoof legitimate phone numbers. As a result, where a legitimate customer's phone number has been spoofed and placed onto a block list, that consumer will be unable to complete phone calls to a consumer utilizing a call blocking technology. This means that the impacted customer will be unable to complete calls to any individual utilizing any block list-supported technologies or services.

During USTelecom's post-hearing discussions with representatives from Primus Canada and NoMoRobo, each entity represented that legitimate customers whose phone number has been spoofed by third parties and placed onto a block list could make arrangements to have their telephone numbers removed from the block list. But if a consumer's phone number is spoofed and placed onto a block list, they will likely have no idea why their calls are not completing to their intended called parties, or who to call in order to resolve the issue. In the event block list technologies are widely deployed by numerous third-party and/or network providers, consumers who are unable to complete phone calls through no fault of their own will be faced with a near-impossible task of figuring out how to fix the problem, or who to contact.

Indeed, some consumers may incorrectly assume that their inability to complete a phone call – or phone calls – is the fault of their current voice provider, or that of the party or parties they are trying to call, being unaware that the party they are trying to reach has subscribed to a call blocking service and that their telephone number has been placed on a block list. Even if the impacted consumer is eventually able to determine that the source of the call blocking is in fact a block list-enabled service, it may be impossible for them to quickly resolve the issue, and vital communications may have been impacted. Under the circumstances, it would be virtually impossible for such a consumer to identify which company is providing the call-blocking service to the party they are trying to call – a problem that will become magnified as more and more such block list-based services enter the market.

---

[17] *See*, PowerPoint Presentation, Henning Schulzrinne, North American Numbering Council (NANC) Meeting, *Preventing CallerID Spoofing*, p. 21, September 18, 2013 (*Schulzrinne Presentation*).

Serious legal and practical issues are also raised regarding a consumer's inability to have their legitimate calls completed for an undetermined period. While both companies indicated that some form of appeal or verification processes is provided, it is of some concern that an innocently impacted consumer would need to go through the time and inconvenience of such a process. Given that impacted consumers would need to spend considerable time identifying the problem and then resolving it, is entirely feasible that they could be unable to complete phone calls to their intended call recipients for days or perhaps longer.

Such a scenario would be problematic for businesses, consumers, and public safety. Legitimate businesses could see their operations and customer relations adversely affected due to their inability to place calls. For consumers, it may not only be a nuisance, but could raise health and safety issues. It would be particularly problematic for public safety agencies that are increasingly utilizing automated robocalls to pass along critical information such as school closings or public safety alerts. As the Commission has previously noted, the inability to complete a phone call can have "dire consequences."[18]

It is thus entirely possible that legitimate and important calls could be blocked by services using block list technologies such as those provided by Primus Canada or NoMoRobo. The Primus Canada model, for example, by design requires a robocaller to press 1 in order to complete the call. Since a public safety entity originating a robocall cannot press 1, the call is effectively blocked. In the NoMoRobo model, if public safety phone numbers are being spoofed and end up on the FTC's Do-Not-Call list, that call will likewise not go through.

While representatives from both Primus and NoMoRobo indicated that such entities could contact the company to be added to a "white list" or removed from the block list, USTelecom was unable to find any such information on either website indicating how to do so. Moreover, it is unlikely that every one of the tens of thousands of local police, fire, education, and public health agencies or districts across the country are likely to contact these two services, much less the untold number of others that may enter the market in the future, even assuming the services themselves all have the wherewithal to handle that volume of white-listing or removals from their block-lists. USTelecom raises this issue not to cast aspersions on the specific companies, but rather to address the serious concerns that could arise in the event that such block list technologies are widely deployed by a large number of either network-based or edge-based providers.

Another vulnerability to which block lists are susceptible is vendetta blacklisting, where an individual or entity nefariously and repeatedly reports a legitimate, non-abusing phone number to the block list based application in an attempt to have that number block-listed. The length of time and effort to be removed from multiple block lists could be harmful to businesses and consumers alike.

---

[18] *FCC Declaratory Ruling*, ¶ 2 (stating "These problems can have dire consequences: Small businesses can lose customers who get frustrated when their calls don't go through. Urgent long distance calls from friends or family can be missed. Schools may be unable to reach parents with critical alerts, including school closings due to extreme weather. And those in need of help may be unable to reach public safety officials.").

Finally, USTelecom was concerned to learn days prior to its launch that NoMoRobo is indiscriminately blocking *all* numbers assigned to a select group of carriers identified by NoMoRobo as "per se" robocallers. To the extent such extrajudicial practices were to be accepted and widely adopted by other edge-based providers offering block list services, its impact on legitimate calls could be significant, since it would block legitimate customers of these entities. At the same time, since a service like NoMoRobo is not subject to common carrier regulation, it is unclear what – if anything – federal and state agencies could do to address such practices.

3. Technologies Necessary for NoMoRobo-Type Services are Not Universally Available

NoMoRobo is a third party application designed specifically for use with VoIP voice platforms where the consumer has access to a calling feature known generically as "simultaneous ring." The consumer is also provided a "dashboard" whereby the simultaneous ring feature – if available – can assign a telephone number to the NoMoRobo server so that it is designated as the first end-user device to receive any incoming call.[19] Technological solutions like the NoMoRobo platform do not generally work on non-VoIP voice platforms, such as Time Division Multiplexing (TDM)-based wireline and wireless networks, where simultaneous ring calling features are generally not available to consumer end users.[20]

Thus, the NoMoRobo service was specifically designed to work with a limited subset of existing VoIP-based voice communications applications. It simply will not work for the vast majority of embedded switch-based voice communications service customers in the United States. In fact, aside from a conversation arranged by USTelecom with Mr. Foss in the days prior to his launch of the NoMoRobo service, we are unaware of any instances where USTelecom's members were contacted pre-launch in order to determine whether its systems application would work in this context. Indeed, the FTC's own rules associated with its Robocall Challenge explicitly required that any proposed solution should not "require changes to all phone switches," and that proposed technologies should work across multiple platforms, including mobile phones, traditional wired lines and VoIP land lines.[21]

---

[19] Telephone Conversation between Aaron Foss, NoMoRobo, and USTelecom Robocall Working Group (September 28, 2013). (*Foss Conversation*).

[20] According to USTelecom estimates for the 4th quarter of 2012, approximately 28% of phone households receive voice services over an IP network from either their cable or ILEC provider where simultaneous ring may be available as an end user feature. In contrast, approximately 34% of phone households receive voice services from either their cable or ILEC provider over a traditional, TDM-based switched network where simultaneous ring is generally not deployed. The remaining 39% of households rely exclusively on wireless providers for their voice network, and simultaneous ring is not a feature generally available in wireless networks.

[21] *See*, FTC Robocall Challenge website, *FTC Robocall Challenge Official Rules*, §§10A(i), (ii) (available at: http://robocall.challengepost.com/details/rules) (visited October 9, 2013).

NoMoRobo's written statement to this Subcommittee states that the service "works on land lines, voice-over-IP and cell phones on all of the major carriers and does not require any additional hardware or software. All that is required by the consumer is a simple, one-time setup, enabling a free feature called simultaneous ring."[22] NoMoRobo may work on VoIP services provided by major carriers where simultaneous ring features are provided as part of the service feature suite, but that does not mean that it will work on non-VoIP services provided by all of the major carriers or that simultaneous ring is a free feature widely available to end user customers of non-VoIP voice communications services. NoMoRobo was apparently designed to launch, at least initially, only with respect to certain VoIP platforms.

Historically, simultaneous ring was not provisioned as an individual consumer end user feature in the TDM-based PSTN because of the additional call signaling load such an end user feature would entail. IP-based communications technology, on the other hand, permits the provisioning of simultaneous ring functionality without the associated signaling and call-set-up challenges facing TDM networks. U.S. carriers are currently in the process of transitioning their TDM networks to IP-based successor networks. Even where it might be possible to deploy simultaneous ring within an existing TDM network, it is not clear whether it could be accomplished while still being able to offer a NoMoRobo-type solution on a cost effective basis to end users.

While this solution may or may not work efficiently in VoIP environments, it is not clear how central office based TDM-networks would affect NoMoRobo's system architecture or cost structure to the extent that a simultaneous ring feature may be available to end users served by any given central office. Just as other companies must often invest in network infrastructure to enable their consumer services utilizing IP networks, NoMoRobo may or may not be required to make the necessary investments to deliver their services as advertised.

U.S. carriers are already at work investing in next generation networks, and are hard at work on the solutions that will make a meaningful and scalable impact on the problem of telephone number spoofing. According to USTelecom industry statistics, the broadband industry has invested nearly $1.2 trillion dollars since 1996. And in recent years, a large and growing majority of that investment has been focused on the deployment of broadband and IP networks. Simultaneous ring is offered as a feature in the VoIP services provided over these new networks. It makes little sense for companies to retrofit transitioning TDM networks with the hardware and software upgrades to enable a third-party application designed for VoIP platforms and that is vulnerable to simple countermeasures such as randomized spoofing. Further, such retrofitting may even pose system architecture challenges and unintended consequences to the NoMoRobo service itself, entailing costs that neither NoMoRobo nor its investors may fully appreciate or have contemplated. As inefficient as it was to deploy simultaneous ring as a consumer calling feature in TDM networks in the past, it is certainly inefficient and inappropriate to do so now.

Finally, while all of our member companies are striving to accelerate the deployment of broadband services to unserved homes across the country, the FCC's 2011 Universal Service Fund (USF) reform order is undermining the ability of small rate-of-return regulated telecom

[22] *Foss Statement*, p. 1.

carriers, serving more than 40% of the nation's land mass, to provide rural consumers with those very services. Instead, the reform order is resulting in declining private sector investment and thus failing to achieve the purposes required by Congress in the Communications Act for "access to communications services reasonably comparable in price and quality to those available in urban areas." We urge the Subcommittee to encourage the FCC to take immediate steps to re-establish predictability, sufficiency, and transparency in the USF program so that these small businesses can resume critical investments in rural broadband. Such investments hold the greatest promise of bringing to rural consumers the IP-enabled voice services that would permit applications like simultaneous ring to function.

4. Consumer Confusion Resulting from the NoMoRobo Product Launch

Despite the inherent limitations in these applications, which were explained by USTelecom members to NoMoRobo prior to product launch,[23] USTelecom understands that consumers with TDM-based wireline or wireless voice service who attempt to initiate the NoMoRobo service eventually land on a NoMoRobo web page that states:

> **Sorry!** None of your carriers currently support Nomorobo.
> **But there is something that you can do!**
> Please call the customer service number below and request that they add *Simultaneous Ringing* to their service so you can finally stop getting robocalls. The more people that call them, the better.
> [Name of Carrier] Customer Service
> 1-877-[Carrier Toll-Free Phone Number]
> *You'll also receive an email when your carrier becomes available*

Each of the three largest carrier members of USTelecom report that their companies have been identified by NoMoRobo in this manner, and, in at least one case, consumers were directed to an incorrect phone number. None of the companies were consulted in regard to this blanket consumer notification.

USTelecom is concerned that American consumers, responding to an appeal for a free service that bears the official symbol (and thus the implicit imprimatur) of the FTC, are at best being importuned to adopt a technology of unknown efficacy and limited scalability with the promise of stopping unwanted robocalls, and at worse, are given unrealistic expectations of an easy solution to a highly complex problem. Moreover, the advisory incorrectly states that the responsibility for the proper functioning of an independent, third-party service lies exclusively with the unaffiliated provider of the underlying voice service.

III. Robocall Mitigation Industry Efforts

As recently noted by the FCC's Chief Technologist, the most effective long term response to the robocall problem is one that industry has already embarked upon: the development of strong caller authentication and authorization mechanisms that are required in all known solutions and

[23] *Foss Conversation.*

that have the potential to scale across an entire country, protecting all consumers rather than a select or targeted few.[24] The industry is actively engaged in the development of a long-term technological solution to this challenge in the form of secure call authentication procedures that can more effectively address the problems posed by hidden, disguised, or spoofed calling party telephone numbers.

The development of standards in this area for use in IP-based communications networks is the priority of the Secure Telephone Identity Revisited (STIR) Working Group recently activated within the Internet Engineering Task Force (IETF). Such solutions will become most effective upon a full transition to IP-based communications networks, a process that is well under way. Public policies that foster investment in broadband and encourage the complete transition to IP-based voice services will hasten the day when the industry will have the kinds of tools it needs to attack illegitimate robocalling.

In the near term, carriers and consumers can continue to employ available technologies that will have some degree of impact on the problem of illegal high volume, auto-dialer initiated calls. Carriers are providing – and will continue to develop – various services consumers can use to help mitigate the robocall problem. These services include basic caller-ID functionality, as well as conditional call-forwarding and anonymous call-blocking. Because the offerings and capabilities of companies are different, consumers are always encouraged to contact their respective service provider in order to identify available resources. These technologies enable carriers to take appropriate responsive action when anomalous mass calling events are identified, including the engagement of law enforcement and regulatory authorities, and they enable most impacted consumers to control which calls they want to receive – provided the telephone numbers have not been spoofed.

[24] *Schulzrinne* Presentation, pp. 18 – 19, 21.