Written Testimony of David Frankel, CEO, ZipDX LLC

17-June 2019

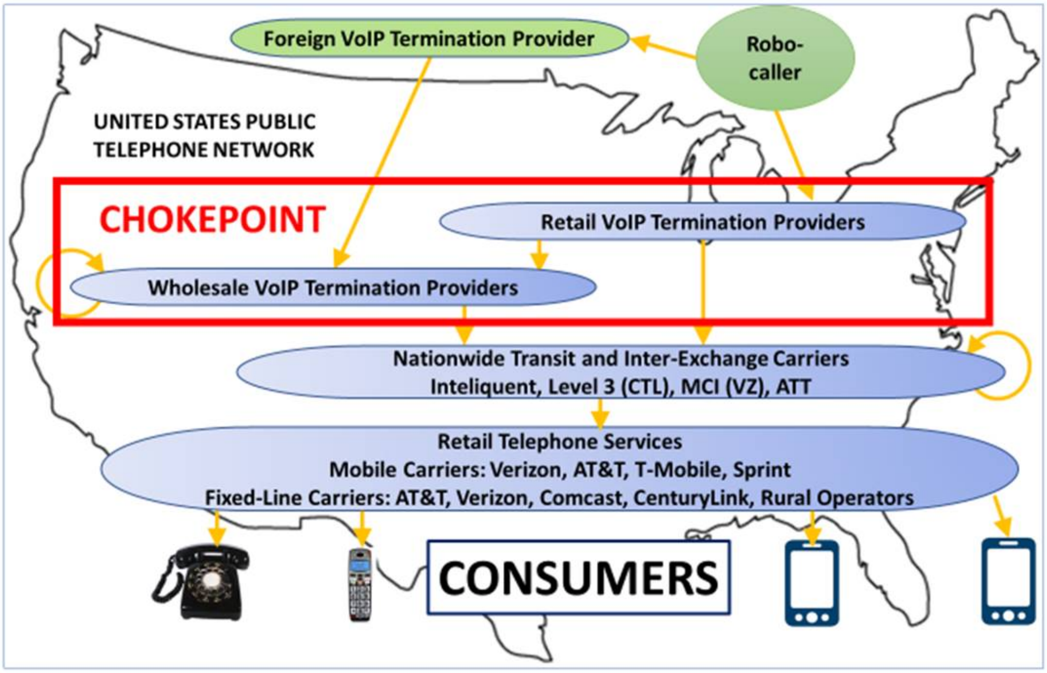
Good morning Senator Collins, Ranking Member Casey, and members of the Special Committee. I am honored to appear before you today. My name is David Frankel; I am the CEO of ZipDX LLC, a provider of specialized telecommunications applications.

While my primary business is not involved in robocalling, legal or otherwise, I became interested in the problem in 2012 and since then have devoted an increasing fraction of my professional time to addressing it.

In my remarks today, I want to share my perspective on illegal robocalls, including how they work technically and commercially, and why they persist. I will attempt to convince you that this is not an intractable problem, but it is one that requires a cooperative, focused, coordinated wide-ranging effort to address.

I have prepared a diagram that illustrates the path taken by most robocalls. The robocaller shown here, located outside the United States, buys "call termination" service from a US- or foreign-based provider. This service, typically using VoIP (Voice-Over-Internet-Protocol) allows the robocaller to initiate his calls and send his digital audio signals to the provider via the internet.

The diagram shows this near the top. The robocaller may come directly to a provider in the United States, or he may go through one or more foreign entities first. Arrangements may be "wholesale" or "retail" and the distinction is imprecise. Buyers of wholesale service often pay lower prices in exchange for higher volumes and are expected to resell the service to others. But the services are often indistinguishable.



Foreign VoIP Termination Provider
Robo-caller
UNITED STATES PUBLIC TELEPHONE NETWORK
CHOKEPOINT
Retail VoIP Termination Providers
Wholesale VoIP Termination Providers
Nationwide Transit and Inter-Exchange Carriers
Inteliquent, Level 3 (CTL), MCI (VZ), ATT
Retail Telephone Services
Mobile Carriers: Verizon, AT&T, T-Mobile, Sprint
Fixed-Line Carriers: AT&T, Verizon, Comcast, CenturyLink, Rural Operators
CONSUMERS

The provider that accepts the calls from the robocaller is designated the Originating Provider. That provider typically buys (via a wholesale arrangement) terminating service from yet another provider, and ultimately the calls are sent to a national transit provider who passes the calls to the providers directly serving the called consumers. These final providers, at the bottom, are Terminating Providers – these are the providers with names familiar to consumers like T-Mobile and Verizon.

Generally, as we move down each level, the aggregate volumes increase and the per-minute prices go down. Each provider earns a small margin on the traffic. But somebody is always paying for the calls; there are commercial agreements at each link in the chain. There is no way to send a call, robo or otherwise, to a subscriber of a US-based consumer telephone service except by arrangement with an originating provider in the United States. That originating provider demands payment for the calls to cover its own costs of sending the calls downstream.

It is not difficult to become a robocaller, nor is it difficult to become an originating provider – and occasionally they are one and the same. There is software and documentation on the internet and people willing to help. You don't have to invest in any equipment, as standard computing resources can be used to process these calls and those resources can easily be rented in "the cloud."

The money involved is not large, even if the number of calls is. Charges are based on connection time after the call is answered. Since most people hang up on robocallers, connection times are very brief, averaging just a fraction of a minute.

The robocaller's approach is to place an enormous number of calls in the hope of finding a handful of respondents that will engage in his pitch. By automating the front end of the process, having a computer place the calls and do an initial screen of the target, he makes much more efficient use of his human agents who only get connected once a potential target has declared their interest.

The business models are similar, whether selling some product or service like a medical device or a timeshare condo, or referring leads for a Medicare supplement plan or a cruise line, or extorting cash by impersonating an IRS or Social Security agent. Each consummated deal will be worth $50 or $250 or $1200 in revenue to the robocaller. His biggest expense is his human agents, who with overhead might cost $20 an hour in the United States, or $40 a day overseas – and likely get paid on commission.

A typical robocaller might snag 50 victims a day, each netting him $100. Working 20 weekdays each month, he collects $100,000. He has ten agents working the phones; perhaps they cost a total of $20,000 per month.

If his agents manage to close one in four people that they talk to, he needs 200 people every day to press 1. If one in a thousand people answer his call and press 1, he'll have to make 200,000 calls daily. That will cost him roughly $400 per day or $8,000 per month

Subtracting his phone and agent expenses from his revenue, our robocaller could be making about 70 grand in profit each month. It's no wonder that this is such a popular endeavor. The originating provider serving the robocaller takes in $8,000 and pays perhaps half that to his downstream provider, so he's making $4,000 per month for allowing the robocaller onto the network.

It's been suggested that the telecom industry likes robocalls because they make money off them. This depends on who you are. For the largest providers at the bottom of our diagram, robocalls are terrible.

Costs to deal with customer complaints, implementing mitigation technologies, and overall damage to the business far outweigh the relatively miniscule revenue generated by the calls. For intermediate providers in the middle, who own and operate complex networks, it's much easier to make money on calls that average two or twenty minutes than twenty seconds. Short-duration traffic congests their network and the customers are fleeting, so they discourage it via pricing strategies and vetting whom they choose to serve.

The providers at the top of the diagram are generally small operations – a few dozen people or perhaps just one or two. Blending in robocall traffic with their other business makes for a nice supplement to their bottom line. By demanding prepayment they avoid credit risk; this is free money.

On a monthly basis, a VoIP provider that originates one hundred million robocalls could net $50,000 to $100,000 in profit. Thirty such operators would account for three billion illegal robocalls, in line with published estimates for current illegal robocall volumes. That's a big boost for these relatively small operations but peanuts in the scale of the US telecommunications business. It amounts to less than one penny per US telephone subscriber.

I want to switch gears now and talk about how we can mitigate these calls, and I'll start with an analogy to hopefully break the monotony of telephony jargon.

Imagine that we find our home infested with ants. They are in the dining room and the laundry room and the family room. Each child is assigned to ant eradication in a given room, and spends several sessions each day searching them out and removing them.

Despite our systemic efforts the problem doesn't abate, so the parents launch a rigorous investigation. Lo, they trace the ants backwards, along the baseboard into the kitchen then up the side of the island to the honey jar, where they discover a huge colony. Alarmed, they post a large sign that states "Federal law prohibits ants from congregating in and around the honey jar."

The children complain that they're falling behind in their homework because patrolling their assigned rooms for ants is consuming an ever-increasing amount of time. The parents launch further investigations and discover another ant colony at a leaking bag of sugar in the baking cupboard. Another sign goes up: "Spilled sugar is off-limits to ants." In passing, we note that the ants are failing to heed our first sign about the honey jar.

The problem continues to worsen. Finally, we hire a professional exterminator, who explains that these are a rogue strain of ants that don't comply with written instructions. He recommends adoption of a new kitchen protocol: All sugary substances must be kept in clean, sealed containers. A small investment in a sugar canister and elimination of the honey jar (which wasn't used anyway) makes a dramatic difference. The exterminator also suggests rinsing ice cream bowls and moving them promptly to the dishwasher, as he anticipates that's going to be the next sweet spot for the ants.

There is a noticeable reduction in the ant population and the children's grades are starting to improve. The patrols continue at a low level because the ants still creep in from the crawlspace and through a hole in a window screen, but the problem is now manageable.

Hopefully my analogy is not too far afield. Stopping the problem at the source – or sources – is much more effective than dealing with it once the ants or calls have dispersed. There is a cost associated with this mitigation, but it is small compared to the alternatives. The most important measure is cost-effectiveness – for a given level of mitigation effort, how many ants or calls are we stopping? There are a finite number of sources and that's where at least some of our attention should be focused.

The best place to stop the illegal traffic is where it first enters the network. This is where it is most concentrated and its source can be identified. As the illegal calls move through the network they disperse and are comingled with other calls, making detection more difficult. Further, if a call is erroneously rejected at the point of entry, the caller is instantly made aware of that and can resolve the issue with their provider. If a call is blocked later, the cause of the block is not readily apparent to the caller and becomes more difficult to resolve.

But the first question to answer is: How do we find the source of the call? The answer should be from the Caller-ID, but takes us immediately to the problem of spoofing, which deserves a history lesson.

Caller-ID was added to the telephone network in the 1970's when digital signaling was introduced. Originating a telephone call meant creating a digital message containing both the destination phone number as well as the originating number; this message was created by the phone company serving the caller.

As digital telephony evolved over the decades, protocols were developed to allow business customers to tell their phone company which specific phone extension was originating a call. For example, if a company's published number was 202-555-1000, the company's PBX could indicate that a specific call was placed from 202-555-1234, so that the called party could know more precisely who was calling and would have a direct call-back number. The phone company would screen the supplied number to make sure it was within the range of numbers assigned to the business.

When telecom became fiercely competitive in the 1990's, business customers began using different telcos for their inbound and outbound calling. A telco providing outbound calling service didn't necessarily know which phone numbers belonged to a given customer, so rather than asking, they turned off the screening function. That was more expedient and suited the fervor of the competitive environment. "Trust but verify" became just "trust."

Now the cat was out of the bag. While legitimate businesses generally have no reason to place calls using calling numbers other than their own, the loose treatment of Caller-ID soon found nefarious applications. This predates VoIP, but VoIP made phone calls ever cheaper and more accessible and spoofing was along for the ride.

The telecom industry has only itself to blame for the spoofing epidemic, but Congress didn't help when it passed the Truth in Caller-ID Act in 2009 and chose the words "with the intent to defraud, cause harm, or wrongfully obtain anything of value." That subjective criteria leaves everybody wondering exactly what is and isn't allowable. The law should have specified only calling numbers "assigned to the caller or used with the permission of the owner." Telephone companies aren't prevented from imposing an objective criterion such as this and some do, but many do not.

Illegal robocallers go out of their way to choose originating providers that allow them to play fast and loose with Caller-ID. When a call arrives at the terminating provider, there is nothing identifying with certainty the caller or the originating provider.

However, responding to the robocall epidemic, the telecom industry now has a process to identify the source of a given call. Providers have long kept records, primarily for billing reasons, of each call handled by their networks. Working cooperatively, each provider, starting with the terminating end, searches its records for the target call and identifies the next provider in the chain that passed the call to it. The process iterates until the originating provider is reached.

Originally this process was entirely manual and was invoked by enforcement authorities issuing subpoenas to each provider in turn; that took weeks to months since there can be four or more providers involved. Now, thanks to some automation and encouragement from each other as well as the FCC, the process can be completed in days or even hours.

By tracing back selected call examples from illegal robocall campaigns, the originating provider(s) can be identified and notified and can take steps to stop the calls. Traceback learns the entire call path, so if the Originating Provider fails to act, the next provider downstream can be engaged to intervene. We don't have to trace back billions or millions of calls. We just need to trace a few examples, and we don't even need all those tracebacks to complete. One successful example can get us to the source.

When an originating provider learns that their platform is being used as a conduit for illegal robocalls, they identify the offending customer from the call examples, and examine all the traffic from that customer. That will inform a strategy for engaging with the customer to eliminate the illegal calls. The provider may also impose network-level constraints, which can include: throttling the rate at which the customer can initiate calls, restricting the number of concurrent calls; and screening the caller-ID value(s) available for the customer's use. These same constraints can and should be applied to all new customers as well. The provider may decide that discontinuance of service is appropriate, especially if violations are on-going. New and existing overseas customers warrant additional scrutiny. Identities of on-going offenders are published; other providers may elect to do extra screening of their calls.

If the Originating Provider fails to mitigate the illegal calls, downstream providers (which are receiving the calls from the Originating Provider) will be wary of continuing to accept that provider's traffic. A downstream provider will notify an offending Originating Provider of terms-of-service and/or acceptable-use-policy violations (which generally prohibit the sending of illegal calls, and often have even more rigorous restrictions). If the traffic continues, the downstream provider will act according to the terms of its contract with the Originating Provider, which can include network constraints like those mentioned above, as well as financial penalties and, in cases where the violations are on-going, termination of service.

Providers that really care about the robocall problem are revising their contracts to insist that their upstream partners cooperate in the fight against illegal robocalls and are prioritizing those revisions to those behaving most problematically.

Every self-respecting US-based telecommunications provider should be contributing to addressing the problem of illegal robocalls. That means participating in traceback efforts. But it also means being prudent about who gets what kind of access to the US telephone network. Very few legitimate entities need the ability to make millions of calls per day. Very few legitimate entities have a valid reason for using a different calling phone number for each call they place. It makes no sense for somebody in India, identified only by a gmail address, to be placing huge numbers of calls that look like they are originating from all over the USA.

US-based providers that allow that to happen are the root cause of our illegal robocall problem.

In closing, I will tell you that efforts to authenticate calls, to educate consumers and provide them with blocking apps, to implement analytics and labeling solutions that warn of bad calls, and to allow legitimate volume callers to rise above the sea of garbage are all good things to do. But I promise you that the most immediate and effective mitigation approach which can rise to the scale necessary to address our current problem rests with the handful of US-based originating providers that are letting these calls onto the network to begin with.

I welcome your questions.