

It's my pleasure to describe to you why what we offer is compliant, is not spoofing, and does not violate the "Truth in Caller ID Act of 2009", which was signed into law on 12-22-10.

To start, here is the law:

<http://www.govtrack.us/congress/billtext.xpd?bill=s111-30> The law says, "(1) IN GENERAL- It shall be unlawful for any person within the United States, in connection with any telecommunications service or IP-enabled voice service, to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, unless such transmission is exempted pursuant to paragraph(3)(B)". The language to key in on is "...misleading or inaccurate caller identification information".

We need to look at the definitions. Section 8 in the law defines "caller identification information" as:

"(A) CALLER IDENTIFICATION INFORMATION- The term 'caller identification information' means information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or IP-enabled voice service". With BellesLink, we allow you to display any telephone number you're leasing from us, or any other number you own or lease, on the caller ID. We don't allow anything else.

Here's Part 1 of an example. Most of the time I work at home. But, I call customers using BellesLink and I display our office number on the caller ID when I call.

Doing so is not spoofing and not a violation of the law. Because first, it's not "misleading or inaccurate caller identification information". Why not? Because I'm calling you from Belles Camp — that's my number. It's registered to me, I own or lease it. Then, when you answer the phone, it's me, from Belles Camp. If you miss the call and call back, that number rings to me. It doesn't matter that I'm at home (because I've set my Belles Camp office number on BellesLink to ring me at home). You called the number back and you reached me at my number. So calling you and displaying "Belles Camp" on the caller ID, even though I'm not in my office, is not illegal and not a violation of any law. Because like I say, I'm calling you from Belles Camp. And two, when you call the number back you can reach me.

For Part 2 of why this is not illegal and not a violation of the law, we need to key in on the definition of "caller identification information". Caller identification information is defined in the law as "...information provided by a caller identification service regarding the telephone number of, or other information regarding the origination of, a call made using a telecommunications service or IP-enabled voice service".

I'm calling you from Belles Camp and if you call the number back it rings to me at home. It doesn't matter if or not I'm in the office. Because, "the telephone number of" on the caller ID is a Belles Camp number. And of course it only follows that "other information regarding the origination of, a call...", the caller ID text (which I'll get to), is in compliance too. Again, because I'm calling from Belles Camp and if you hit redial you get me at Belles Camp. My location has nothing to do with this.

So how does this relate to BellesLink? It's the same premise. If you activate a number from BellesLink and then that number rings at your desk or somewhere else such as your phone lines or equipment, as long as you can be reached at that number, you're not breaking the law. Because the number you activated is yours and you pay for it. So therefore, it's the "telephone number of".

We also offer caller ID name, the ability for you to set the caller ID text that displays with each call. By displaying a caller ID name on the caller ID, that's also not a violation. Because, that caller ID name is "other information regarding the origination of, a call...".

Here's an example:

You called someone and displayed one of our local numbers along with the caller ID text on the caller ID. You set the caller ID text to "Repo Company". You left a message, "I'm calling from The Repossession Company, please call me back, I have an important matter to discuss with you...".

Have you broken the law? No, not as long as you are a repossession company. Your "caller identification information" was neither "misleading or inaccurate". And, when someone calls you back, you can be reached at the number you left. Not only that, it answered to what you left in your voicemail -- "The Repossession Company". So, "the telephone number of, or other information regarding the origination of, a call..." was accurate.

Note that this law doesn't preclude you from using an alias. In fact it doesn't even address that concept. Set that aside. But now keep in mind that the law allows you to block your caller identification information. See this: "(2) PROTECTION FOR BLOCKING CALLER IDENTIFICATION INFORMATION. Nothing in this subsection may be construed to prevent or restrict any person from blocking the capability of any caller identification service to transmit caller identification information".

One could easily make the argument that by blocking your caller identification information and displaying one of our local numbers instead, all you're doing is blocking your caller ID -- which the law allows for.

Here's another good example. When you travel and make a call using your cell phone, the caller ID still shows as coming from your home coverage area. Are you spoofing? No, of course not. The law makers wrote the law to take situations like this one, and the legitimate needs of telecommunications services like ours into account. Otherwise, anyone who travels out of their home coverage area and makes a call would be spoofing.

The Truth in Caller ID Act of 2009 was not designed to block you from using telecommunications services such as ours. It was only designed, to keep people from displaying phone numbers on the caller ID that the caller has no right to use and that the caller cannot be reached at.

Now review the letter from Department of Justice included. See the bottom of page 1. It says, "Nor should spoofing be understood to include transmitting a number related to a private branch exchange (PBX, tech term for a phone system) or the main telephone number of a business's network in place of an extension". When you make calls using our local numbers, you're making calls using a "PBX" — the BellesLink PBX.

This letter was sent to the FCC as part of the FCC's review of the law on June 22nd, 2011. Because, the law needs to accommodate the legitimate needs of services like Vonage, or other VOIP (voice over internet protocol) services. They're not spoofers and neither are we. They're about compliance, so are we. Here's the language the FCC added to accommodate these types of services:

1. Information regarding the origination (of a call). The definitions of "caller identification information" and "caller identification service" in the Act and in the rules we adopt today both use the phrase "the telephone number of, or other information regarding the origination of, a call." We define "information regarding the origination" to mean any: (1) telephone number; (2) portion of a telephone number, such as an area code; (3) name; (4) location information; (5) billing number information, including charge number, ANI, or pseudo-ANI; or (6) other information regarding the source or apparent source of a telephone call. The definition we adopt today mirrors the proposed definition, but adds "billing number information including charge number, ANI, or pseudo-ANI" to the types of information that constitute "information regarding the origination." We add these types of information to the definition of "information regarding the origination" in response to commenters' concerns about the importance of transmission of accurate billing information, including charge number, ANI and pseudo- ANI, to caller identification services used by emergency services providers.

The FCC added this language so that services like Vonage, and BellesLink, that allow users to activate a local number anywhere they offer numbers, aren't included as spoofers. For example let's say I have an ad in the Miami paper selling Widgets. I can hop on Vonage's site today, grab a number in Miami. When someone calls the number from Miami, it rings to me in CO. Then when I make calls, I need to be able to display my Miami Vonage number on the caller ID. The number is mine, I'm paying for it, I'm selling Widgets. It doesn't matter if I'm in Miami or not. It only matters whether or not the Miami number is mine, that I can be reached at it and I'm selling Widgets. It is, I can, I am. Am I a spoofer? No, of course not.

Another example is call centers. When you get a call from a sales person at say Zappos.com (online shoe retailer) your caller ID shows "Zappos" and the number — maybe a number in Seattle. When you call the number back you get someone at Zappos.com. But most likely, that person is not working in Seattle. Maybe they're in India, where just about every other call center agent seems to be working these days. Is Zappos.com spoofing? No, they're not.

Your use of local numbers as I've outlined is compliant and it's not spoofing. It's no different than the examples such as these. Not only that, the DOJ is specifically telling the FCC to make sure the law cannot be interpreted that "transmitting a number related to a private branch exchange (PBX)" would be in violation. Again, when you make calls from our equipment -- you're making calls from a PBX.

The law makers are way ahead on this one because they've heard from the call centers, from online retailers, and from other legitimate telecommunications providers such as us.

There's one other key point here, that demonstrates how well we understand things and how on top of things we are.

See the top of page 4, in the DOJ letter. Note where the DOJ is recommending that "...caller ID spoofing services to make a good faith effort to verify that a user has the authority to use the substituted number, such as placing a one-time verification call to that number".

We allow you to use other numbers for the caller ID other than BellesLink numbers. We've been doing this since before the day after the law went into affect, 12-23-10.

We use what's called a two step verification process. If you want to place a call in BellesLink using another number for the caller ID other than a BellesLink number, to verify you have the legitimate right to display a number other than ours on the caller ID we place a call to that number. The person answering the phone has to enter a code displayed on the BellesLink website.

Or in other words, we were following the best practice outlined in the DOJ letter — well before their letter came out! But of course we're not a "spoofing service".

I hope you feel this is proof positive, that you're in the right place with BellesLink. And, I hope you feel it covers that law makers fully understood they needed to allow the legitimate uses of telecommunications services such as BellesLink's. I hope you agree it's clear they understand that you or I should be able to use a number in some other city, and not have to be in that city to make a call.

Or in other words I hope you see they fully understand, recognize, support, and do not want to impede legitimate services such as BellesLink.

Finally, I hope this gives you 110% confidence in BellesLink's commitment to compliance. We have a combined 100 years of experience, we're the experts. You can build your operations around BellesLink.

Sincerely,  
Paul Kulas  
Head Belle Ringer  
Belles Camp Communications LLC



U.S. Department of Justice

Criminal Division

Assistant Attorney General

Washington, D.C. 20530

January 26, 2011 FILED/ACCEPTED

JAN 28 2011

Federal Communications Commission  
Office of the Secretary

Marlene H. Dortch, Secretary  
Federal Communications Commission  
Office of the Secretary  
445 12th Street, SW  
Room TW-A325  
Washington, DC 20554

Dear Ms. Dortch:

On December 22, 2010, the President signed Public Law No. 111-331, the Truth in Caller ID Act of 2009, which prohibits the use of false caller ID information for the purpose of committing fraud or causing harm. This letter expresses the views of the United States Department of Justice regarding the public safety and law enforcement concerns that the Federal Communications Commission should address in the implementing regulations that the Act directs the Commission to adopt. We believe that the Commission can act to protect public safety and to promote the effective and efficient enforcement of our Nation's laws by adopting regulations that encourage the responsible provision of caller ID spoofing services.

**I. Background**

The Truth in Caller ID Act addresses caller ID spoofing, i.e., altering the telephone number displayed to the recipient of a telephone call to a number different than the caller's actual telephone number.<sup>1</sup> Although caller ID spoofing once required special equipment and/or a relatively high degree of technical sophistication, there are now widely available services that make caller ID spoofing as simple and inexpensive as placing a call with a traditional telephone calling card.

The widespread availability of caller ID spoofing services is a significant facilitator of criminal activity and a substantial threat to public safety. Numerous examples from around the country demonstrate these concerns, including the incidents described below:

---

<sup>1</sup> The notion of spoofing does not include caller ID *blocking* – i.e. preventing any caller ID from being displayed, a capability that telecommunications carriers generally are required to support. See 47 C.F.R. § 64.1601(b). Nor should spoofing be understood to include transmitting a number related to a private branch exchange (PBX) or the main telephone number of a business's network in place of an extension.

- Spoofed caller ID services have enabled a particularly insidious form of fraud known as “swatting.” Swatting refers to the practice of placing false emergency calls to law enforcement for the purpose of eliciting a response from the Special Weapons and Tactics (“SWAT”) team, usually as a means of revenge. In one of the largest swatting cases to date, Stuart Rosoff and a number of co-conspirators pled guilty to participating in a swatting conspiracy that targeted more than 100 victims. Using a spoofing service, Rosoff and his co-conspirators were able to place calls to the police that appeared to originate from the home telephone of their chosen victim. In these calls, one of the conspirators would identify himself to police as a member of the targeted family. The imposter would then tell police that he had shot and killed several members of the family and was holding the remaining family members hostage. Believing the emergency to be real, law enforcement would respond on an emergency basis, leading to dangerous confrontations between heavily armed police officers and the innocent victims of the “swatting” incident. At least two injuries resulted.
- Caller ID spoofing services are often used in connection with stalking and harassment. For example, in 2008, Danielle Zimmer and Carmen Venezia pled guilty to harassment and making terrorist threats. Zimmer and Venezia used a spoofing service to place 13 different calls to the cell phones of Zimmer’s co-workers. The calls were placed in the middle of the night and, as a result of a spoofing service, appeared to originate from the victim’s home telephone number. During the calls, Venezia would inform the victims that he had broken into their home and was watching them.
- Caller ID spoofing services are also widely used by identity thieves. In one long-running scam, members of the public are called from a spoofed telephone number associated with the local court. Call recipients are told they missed their scheduled jury duty and are threatened with prosecution. The victims are then ordered to provide personally identifying information, including their Social Security number.
- Identity thieves also use caller ID spoofing services to access cellular telephone voicemail. When a call appears to originate from a user’s cellular telephone, most cellular providers do not require a password in order to access the user’s voicemail account. As a result, identity thieves are able to access most cellular telephone voicemail systems simply by spoofing the victim’s cellular telephone number. According to news reports, more than 50 voicemail accounts – including several belonging to celebrities – were accessed in this manner in a 2006 incident.

Widespread availability of caller ID spoofing services also enables criminals to more effectively hide their activities from law enforcement and significantly complicates evidence collection by law enforcement.

## II. Recommendations

### 1. Rules Governing Providers of Caller ID Spoofing Services

Chairman Richard Boucher, whose subcommittee reported the House companion bill, introduced the bill on the House floor. At that time, he elaborated on the rules that Congress expects the FCC to adopt pursuant to the legislation:

In the rulemaking that the FCC will conduct pursuant to new subsection 227(e)(3) of the Communications Act, the committee anticipates that the commission will consider imposing obligations on entities that provide caller ID spoofing services to the public. The widespread availability of caller ID spoofing services presents a significant potential for abuse and hinders law enforcement's ability to investigate crime.

The prohibition in this bill on the use of those services with the intent to defraud, cause harm, or wrongfully obtain anything of value could be of limited value if entities continue to provide those services without making any effort to verify their users' ownership of the phone number that is being substituted.<sup>2</sup>

Chairman Boucher's floor statement upon passage of the Act also reflects the expectations of the full House Energy and Commerce Committee, which included a nearly identical statement in its report on the companion bill, H.R. 1258.<sup>3</sup>

As Representative Boucher explained, in order to fulfill the purpose of the Truth in Caller ID Act, it is necessary to ensure that caller ID spoofing services are not havens for criminal activity. Although outlawing the use of caller ID spoofing services for criminal purposes is a good first step, it is unlikely that criminals who are already intent on breaking the law are going to be significantly deterred from spoofing caller ID by the potential for an additional criminal charge. By directing the Commission to adopt rules to implement the Act, Congress expressed its intent that the Commission adopt such regulations as it finds necessary and feasible to address the problems caused by the widespread public availability of caller ID spoofing services.

The Department of Justice shares Congress' concern about the ready availability of services that allow users to spoof telephone numbers with which they have no association

---

<sup>2</sup> 156 Cong. Rec. H8378 (daily ed. Dec. 15, 2010) (statement of Rep. Boucher), available at [http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=H8378&dbname=2010\\_record](http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=H8378&dbname=2010_record).

<sup>3</sup> See House Comm. on Energy and Commerce, Truth in Caller ID Act of 2010, H.R. Rep. No. 461, 111<sup>th</sup> Cong., 2d Sess. 8 (2010), available at <http://thomas.loc.gov/cgi-bin/cpquery/T?&report=hr461&dbname=111&>.

whatsoever. Accordingly, the Commission should consider the feasibility of requiring public providers of caller ID spoofing services to make a good-faith effort to verify that a user has the authority to use the substituted number, such as by placing a one-time verification call to that number. In addition, the Commission should consider technical standards that would permit call recipients to determine whether caller ID information has been altered, and allow law enforcement to trace such calls to the true originating telephone number with appropriate authority.

## 2. The Law Enforcement and Court Orders Exceptions

Section 2 of the Act provides that “lawfully authorized investigative, protective, or intelligence activity” of a law enforcement or intelligence agency are not to be affected by the prohibitions within the Act. To ensure that lawful investigations are not impeded, the Act also specifically directs the Commission to include in its regulations an exemption for law enforcement agencies and court orders. *See* § 227(e)(3)(B)(ii)(I), (II).

The exemption for law enforcement agencies can be modeled on many existing statutory exemptions for the same purposes, including sections 1028 and 1030 of Title 18 of the United States Code. The Department recommends the following language:

*(a) This subsection does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.*

*(b) This subsection does not prohibit any activity in connection with a court order that specifically authorizes the use of caller identification manipulation.*

## 3. The Definition of “IP-Enabled Voice Service”

Finally, the Act defines the offense using the phrase “in connection with any telecommunications service or IP-enabled voice service.” *See* § 227(e)(1). The Act provides that the term “IP-enabled voice service has the meaning given that term by section 9.3 of the Commission’s regulations (47 C.F.R. 9.3), as those regulations may be amended by the Commission from time to time.” § 227(e)(8)(C). Given that section 9.3 does not currently define that term, the Commission should adopt a definition consistent with the public interest and with the purpose of the legislation. Such a definition could be modeled on the one already existing in 18 U.S.C. § 1039(h)(4):

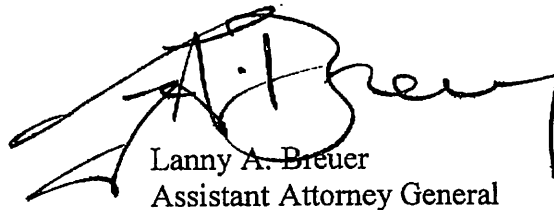
**IP-enabled voice service.** - The term “IP-enabled voice service” means the provision of real-time voice communications offered to the public, or such class of users as to be effectively available to



the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, (whether part of a bundle of services or separately) with interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network, or a successor network.<sup>4</sup>

The Department looks forward to working with the Commission on its adoption of rules as required by the Truth in Caller ID Act.

Respectfully submitted,



Lanny A. Breuer  
Assistant Attorney General

---

<sup>4</sup> 18 U.S.C. § 1039(h)(4) (defining the term for purposes of implementing the Telephone Records and Privacy Protection Act of 2006, which protects confidential phone records information).